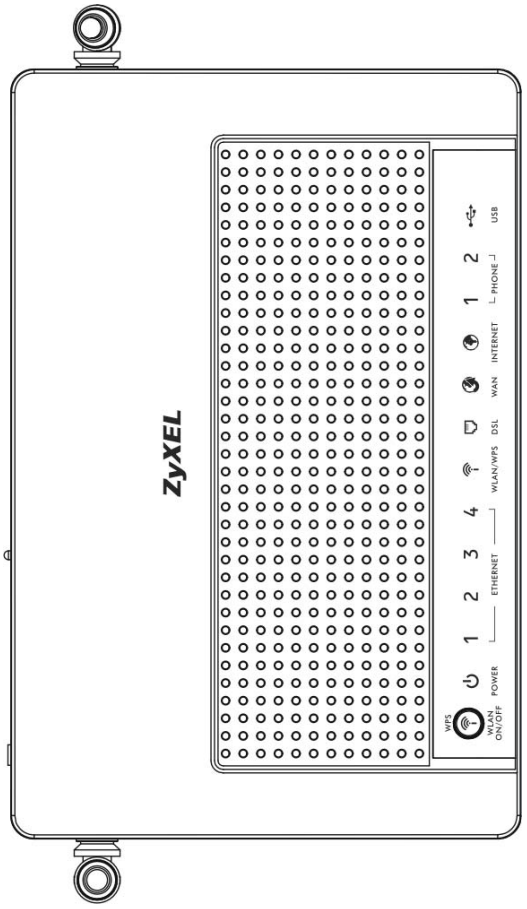
P-2612HNU-Fx

802.11n ADSL2+ VoIP IAD

User's Guide



Default Login Details

IP Address	https://192.168.1.1
User Name	Admin account: admin User account: user
Password	Admin account: 1234 User account: 1234

Firmware Version 3.0
Edition 1, 2/2010

ZyXEL

www.zyxel.com

Copyright © 2010
ZyXEL Communications Corporation

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the ZyXEL Device using the web configurator.

Related Documentation

- Quick Start Guide

  The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access.

- Support Disc

  Refer to the included CD for support documents.

Documentation Feedback

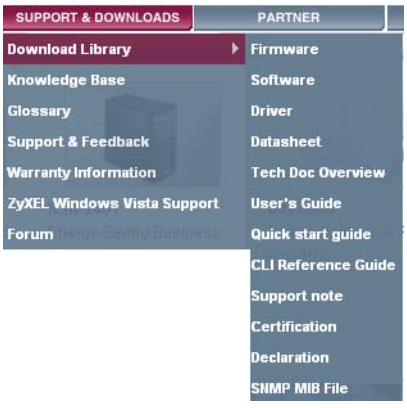
Send your comments, questions or suggestions to: techwriters@zyxel.com.tw

Thank you!

The Technical Writing Team, ZyXEL Communications Corp.,
6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 30099, Taiwan.

Need More Help?

More help is available at www.zyxel.com.



- Download Library

  Search for the latest product updates and documentation from this link. Read the Tech Doc Overview to find out how to efficiently use the User Guide, Quick Start Guide and Command Line Interface Reference Guide in order to better understand how to use your product.

- Knowledge Base

  If you have a specific question about your product, the answer may be here. This is a collection of answers to previously asked questions about ZyXEL products.

- Forum

  This contains discussions on ZyXEL products. Learn from others who use ZyXEL products and share your experiences as well.

Customer Support

Should problems arise that cannot be solved by the methods listed above, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device.

See http://www.zyxel.com/web/contact_us.php for contact information. Please have the following information ready when you contact an office.

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

> **Warnings tell you about things that could harm you or your device.**

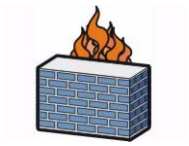
Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The P-2612HNU-Fx may be referred to as the "ZyXEL Device", the "device", the "system" or the "product" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The ZyXEL Device icon is not an exact representation of your device.

ZyXEL Device	Computer	Notebook computer
Server	DSLAM	Firewall 
Telephone	Switch	Router

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.

Contents Overview

Introduction 19

Introducing the ZyXEL Device 21
Introducing the Web Configurator 27
Tutorial 33

Advanced 83

Status Screens 85
WAN Setup 97
LAN Setup 121
Wireless LAN 129
Network Address Translation (NAT) 149
Voice 157
File Sharing 183
Media Server 193
Print Server 195
MAC Filter 201
Firewall 203
Certificates 209
Static Route 219
Quality of Service (QoS) 223
Dynamic DNS Setup 237
Service Control 239

Maintenance, Troubleshooting and Specifications 241

System 243
Logs 247
Tools 253
..... 263
Diagnostic 265
Account 269
Troubleshooting 271
Product Specifications 279

Appendices and Index 291

Table of Contents

About This User's Guide 3

Document Conventions 5

Safety Warnings 7

Contents Overview 9

Table of Contents 11

Part I: Introduction 19

Chapter 1
Introducing the ZyXEL Device 21

1.1 Overview 21
1.2 Applications for the ZyXEL Device 21
1.2.1 Internet Access 22
1.2.2 VoIP Features 23
1.2.3 ZyXEL Device's USB Support 23
1.3 Ways to Manage the ZyXEL Device 23
1.4 Good Habits for Managing the ZyXEL Device 24
1.5 LEDs (Lights) 24
1.6 The RESET Button 26
1.7 The WPS/WLAN Button 26

Chapter 2
Introducing the Web Configurator 27

2.1 Overview 27
2.1.1 Accessing the Web Configurator 27
2.2 Web Configurator Main Screen 28
2.2.1 Title Bar 29
2.2.2 Navigation Panel 29
2.2.3 Main Window 32
2.2.4 Status Bar 32

Chapter 3
Tutorial 33

3.1 Overview 33

3.2 Setting Up Your DSL Connection 33
3.3 How to Set up a Wireless Network 38
3.3.1 Example Parameters 38
3.3.2 Configuring the AP 38
3.3.3 Configuring the Wireless Client 41
3.4 Setting Up NAT Port Forwarding 47
3.5 How to Make a VoIP Call 48
3.5.1 VoIP Calls With a Registered SIP Account 48
3.6 Using the File Sharing Feature 50
3.6.1 Set Up File Sharing 50
3.6.2 Access Your Shared Files From a Computer 51
3.7 Using the Media Server Feature 52
3.7.1 Configuring the ZyXEL Device 53
3.7.2 Using Windows Media Player 53
3.7.3 Using a Digital Media Adapter 56
3.8 Using the Print Server Feature 58
3.9 Configuring the MAC Address Filter 73
3.10 Configuring Static Route for Routing to Another Network 74
3.11 Configuring QoS Queue and Class Setup 77
3.12 Access the ZyXEL Device Using DDNS 80
3.12.1 Registering a DDNS Account on www.dyndns.org 81
3.12.2 Configuring DDNS on Your ZyXEL Device 81
3.12.3 Testing the DDNS Setting 82

Part II: Advanced 83

Chapter 4
Status Screens 85

4.1 Status Overview 85
4.2 DHCP Client List 90
4.3 WLAN Client List 91
4.4 Packet Statistics 92
4.5 VoIP Statistics 93

Chapter 5
WAN Setup 97

5.1 Overview 97
5.1.1 What You Can Do in this Chapter 97
5.1.2 What You Need to Know 98
5.1.3 Before You Begin 99
5.2 The Layer 2 Interface Screen 99

5.2.1 Layer 2 Interface Configuration 101
5.3 The Internet Connection Screen 103
5.3.1 WAN Connection Configuration 105
5.4 Technical Reference 113

Chapter 6
LAN Setup 121

6.1 Overview 121
6.1.1 What You Can Do in this Chapter 121
6.1.2 What You Need To Know 122
6.1.3 Before You Begin 122
6.2 The IP Screen 122
6.3 DHCP Server Screen 123
6.4 The Client List Screen 124
6.5 Technical Reference 126

Chapter 7
Wireless LAN 129

7.1 Overview 129
7.1.1 What You Can Do in this Chapter 129
7.1.2 What You Need to Know 130
7.1.3 Before You Begin 133
7.2 The Wireless LAN General Screen 133
7.3 The Security Screens 136
7.3.1 No Security 137
7.3.2 Static WEP/Shared WEP Encryption 137
7.3.3 WPA-PSK/WPA2-PSK Authentication 139
7.3.4 WPA/WPA2 Authentication 140
7.4 The QoS Screen 142
7.5 WPS 143
7.6 Scheduling Screen 145
7.7 Association List Screen 147
7.8 Wireless LAN Technical Reference 148

Chapter 8
Network Address Translation (NAT) 149

8.1 Overview 149
8.1.1 What You Can Do in this Chapter 149
8.1.2 What You Need To Know 149
8.2 Port Forwarding 150
8.2.1 Configuring the Port Forwarding Screen 151
8.2.2 The Port Forwarding Edit Screen 153
8.3 NAT Technical Reference 154

8.3.1 NAT Definitions 154
8.3.2 What NAT Does 155
8.3.3 How NAT Works 155

Chapter 9
Voice 157

9.1 Overview 157
9.1.1 What You Can Do in this Chapter 157
9.1.2 What You Need to Know 158
9.1.3 Before You Begin 159
9.2 The SIP Service Provider Screen 159
9.2.1 Dial Plan Rules 163
9.3 The SIP Account Screen 165
9.4 The Analog Phone Screen 169
9.5 The Phone Region Screen 170
9.6 The Speed Dial Screen 170
9.7 SIP Technical Reference 172
9.7.1 VoIP 172
9.7.2 SIP 172
9.7.3 Quality of Service (QoS) 178
9.7.4 Phone Services Overview 179

Chapter 10
File Sharing 183

10.1 Overview 183
10.1.1 What You Can Do in this Chapter 183
10.1.2 What You Need to Know 184
10.1.3 Before You Begin 184
10.2 The Share Configuration Screen 185
10.2.1 Share Configuration Add Screen 187
10.2.2 Share Configuration Edit Screen 189
10.3 The Account Management Screen 190
10.3.1 Account Management Add or Edit Screen 191

Chapter 11
Media Server 193

11.1 Overview 193
11.1.1 What You Can Do 193
11.1.2 What You Need to Know in this Chapter 193
11.2 The Media Server Screen 194

Chapter 12
Print Server 195

12.1 Overview 195
12.1.1 What You Can Do in this Chapter 195
12.1.2 What You Need to Know 195
12.1.3 Before You Begin 196
12.2 The Print Server Screen 197
12.3 Technical Reference 197

Chapter 13
MAC Filter 201

13.1 Overview 201
13.1.1 What You Can Do in this Chapter 201
13.1.2 What You Need to Know 201
13.2 MAC Filter Screen 202

Chapter 14
Firewall 203

14.1 Overview 203
14.1.1 What You Can Do in the Firewall Screens 203
14.1.2 What You Need to Know About Firewall 203
14.2 The Firewall Screen 204
14.3 Firewall Technical Reference 206
14.3.1 Firewall Rules Overview 206
14.3.2 Guidelines For Enhancing Security With Your Firewall 206
14.3.3 Security Considerations 207

Chapter 15
Certificates 209

15.1 Overview 209
15.1.1 What You Can Do in this Chapter 209
15.1.2 What You Need to Know 209
15.1.3 Verifying a Certificate 211
15.2 My Certificates 212
15.3 Trusted CAs 214
15.4 Trusted CA Import 215
15.5 Trusted CA Details 216

Chapter 16
Static Route 219

16.1 Overview 219
16.1.1 What You Can Do in this Chapter 219
16.2 Configuring Static Route 220
16.2.1 Static Route Add/Edit 221

Chapter 17
Quality of Service (QoS) 223

17.1 Overview 223
17.1.1 What You Can Do in this Chapter 223
17.1.2 What You Need to Know 224
17.2 The QoS General Screen 224
17.3 The Queue Setup Screen 226
17.3.1 Adding/Editing a QoS Queue 227
17.4 The Class Setup Screen 227
17.4.1 QoS Class Add/Edit 229
17.5 The QoS Monitor Screen 233
17.6 QoS Technical Reference 233
17.6.1 IEEE 802.1Q Tag 234
17.6.2 IP Precedence 234
17.6.3 DiffServ 234

Chapter 18
Dynamic DNS Setup 237

18.1 Overview 237
18.1.1 What You Can Do in the DDNS Screen 237
18.1.2 What You Need To Know About DDNS 237
18.2 Configuring Dynamic DNS 238

Chapter 19
Service Control 239

19.1 Overview 239
19.1.1 What You Can Do in this Chapter 239
19.1.2 What You Need to Know 239
19.2 The Service Control Screen 240

Part III: Maintenance, Troubleshooting and Specifications 241

Chapter 20
System 243

20.1 Overview 243
20.1.1 What You Can Do in this Chapter 243
20.1.2 What You Need to Know 243
20.2 The System General Screen 244
20.3 The Time Setting Screen 245

Chapter 21
Logs 247

21.1 Overview 247
21.1.1 What You Can Do in this Chapter 247
21.1.2 What You Need To Know 247
21.2 The View Log Screen 248
21.3 The Log Settings Screen 249
21.4 Log Descriptions 250

Chapter 22
Tools 253

22.1 Overview 253
22.1.1 What You Can Do in this Chapter 253
22.1.2 What You Need To Know 253
22.1.3 Before You Begin 255
22.2 Firmware Upgrade Screen 255
22.3 The Configuration Screen 256
22.4 Restart 259
22.5 Technical Reference 260
22.5.1 Tool Examples 260
..... 263

Chapter 23
Diagnostic 265

23.1 Overview 265
23.1.1 What You Can Do in the Diagnostic Screens 265
23.2 The General Diagnostic Screen 265

Chapter 24
Account 269

24.1 Overview 269
24.2 Admin/Account Screen 269

Chapter 25
Troubleshooting 271

25.1 Overview 271
25.2 Power, Hardware Connections, and LEDs 271
25.3 ZyXEL Device Access and Login 272
25.4 Internet Access 274
25.5 Phone Calls and VoIP 275
25.6 Multiple SIP Accounts 276
25.6.1 Outgoing Calls 276
25.6.2 Incoming Calls 277
25.7 USB Device Connection 278

Chapter 26
Product Specifications 279

Part IV: Appendices and Index 291

Appendix A IP Addresses and Subnetting 293

Appendix B Setting Up Your Computer's IP Address 305

Appendix C Pop-up Windows, JavaScripts and Java Permissions 335

Appendix D Wireless LANs 345

Appendix E Common Services 369

Appendix F Open Software Announcements 373

Appendix G Legal Information 397

Index 399

PART I
Introduction

Introducing the ZyXEL Device (21)

Introducing the Web Configurator (27)

Tutorial (33)

1

Introducing the ZyXEL Device

1.1 Overview

The ZyXEL Device is an ADSL2+ Integrated Access Device (IAD) that combines an ADSL2+ router with Voice over IP (VoIP) communication capabilities to allow you to use a traditional analog telephone to make Internet calls. By integrating DSL and NAT, you are provided with ease of installation and high-speed, shared Internet access. The ZyXEL Device is also a complete security solution with a robust firewall and content filtering.

Please refer to the following description of the product name format.

- "H" denotes an integrated 4-port hub (switch).
- "N" denotes wireless functionality, including 802.11n mode. There is an embedded mini-PCI module for IEEE 802.11b/g/n wireless LAN connectivity.
- "U" denotes a USB port used to share files via a USB memory stick or a USB hard drive. The ZyXEL Device can also function as a print server with an USB printer connected.
- Models ending in "1", for example P-2612HNU-F1, denote a device that works over the analog telephone system, POTS (Plain Old Telephone Service). Models ending in "3" denote a device that works over ISDN (Integrated Services Digital Network) or T-ISDN (UR-2).

Only use firmware for your ZyXEL Device's specific model. Refer to the label on the bottom of your ZyXEL Device.

See the chapter on product specifications for a full list of features.

1.2 Applications for the ZyXEL Device

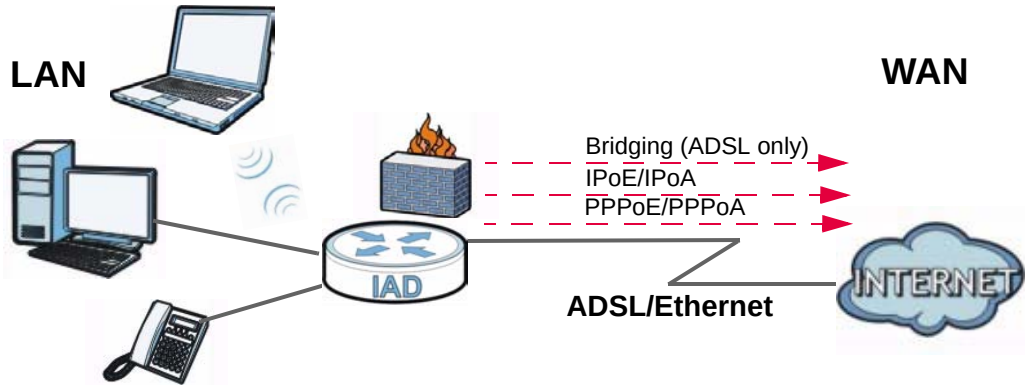
Here are some example uses for which the ZyXEL Device is well suited.

1.2.1 Internet Access

Your ZyXEL Device provides shared Internet access by connecting the DSL port to the **DSL** or **MODEM** jack on a splitter or your telephone jack. If you prefer not to use a DSL line and you have another broadband modem or router (such as ADSL) available, you can push the **DSL / WAN** switch (on the rear panel) to the **WAN** side and connect the **WAN** port to the broadband modem or router. This way, you can access the Internet via an Ethernet connection and still use the QoS, Firewall and VoIP functions on the ZyXEL Device.

Computers can connect to the ZyXEL Device's LAN ports (or wirelessly).

Figure 1 ZyXEL Device's Internet Access Application



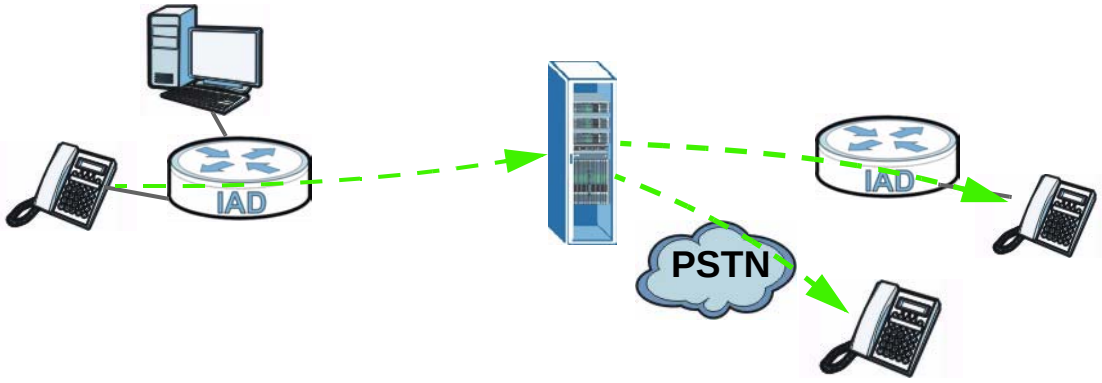
You can also configure firewall on the ZyXEL Device for secure Internet access. When the firewall is on, all incoming traffic from the Internet to your network is blocked unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you can safely browse the Internet and download files.

Use QoS to efficiently manage traffic on your network by giving priority to certain types of traffic and/or to particular computers. For example, you could make sure that the ZyXEL Device gives voice over Internet calls high priority, and/or limit bandwidth devoted to the boss's excessive file downloading.

1.2.2 VoIP Features

You can register up to 2 SIP (Session Initiation Protocol) accounts and use the ZyXEL Device to make and receive VoIP telephone calls:

Figure 2 ZyXEL Device's VoIP Application

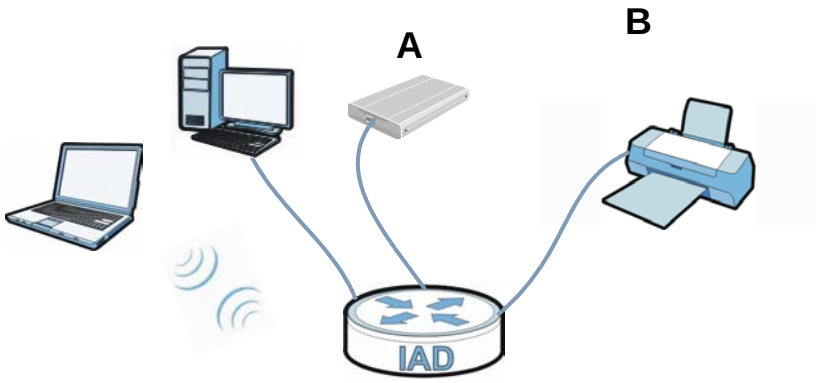


The ZyXEL Device sends your call to a VoIP service provider's SIP server which forwards your calls to either VoIP or PSTN phones.

1.2.3 ZyXEL Device's USB Support

Use the built-in USB 2.0 port to share files via a USB memory stick or a USB hard drive (**A**). Alternatively, you can add a USB printer (**B**) and make it available on your local area network.

Figure 3 USB File Sharing or Print Server Application



1.3 Ways to Manage the ZyXEL Device

Use any of the following methods to manage the ZyXEL Device.

- Web Configurator. This is recommended for everyday management of the ZyXEL Device using a (supported) web browser.
- Command Line Interface. Line commands are mostly used for troubleshooting by service engineers.
- FTP for firmware upgrades and configuration backup/restore.

1.4 Good Habits for Managing the ZyXEL Device

Do the following things regularly to make the ZyXEL Device more secure and to manage the ZyXEL Device more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the ZyXEL Device to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the ZyXEL Device. You could simply restore your last configuration.

1.5 LEDs (Lights)

The following graphic displays the labels of the LEDs.

Figure 4 LEDs on the Top of the Device

None of the LEDs are on if the ZyXEL Device is not receiving power.

Table 1 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
POWER	Green	On	The ZyXEL Device is receiving power and ready for use.
	Red	On	The ZyXEL Device detected an error while self-testing, or there is a device malfunction.
		Off	The ZyXEL Device is not receiving power.

Table 1 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
ETHERNET 1-4	Green	On	The ZyXEL Device has an Ethernet connection with a device on the Local Area Network (LAN).
		Blinking	The ZyXEL Device is sending/receiving data to /from the LAN.
		Off	The ZyXEL Device does not have an Ethernet connection with the LAN.
WPS/ WLAN	Green	On	The wireless network is activated and is operating in IEEE 802.11b/g mode.
		Blinking	The ZyXEL Device is communicating with other wireless clients.
		Off	The wireless network is not activated.
DSL	Green	On	This light applies when the ZyXEL Device is in DSL WAN mode. The DSL line is up.
		Blinking	The ZyXEL Device is initializing the DSL line.
		Off	The DSL line is down.
WAN	Green	On	This light applies when the ZyXEL Device is in Ethernet WAN mode. The ZyXEL Device has an Ethernet connection with a device on the WAN.
		Blinking	The ZyXEL Device is sending/receiving data to/from the WAN.
		Off	The ZyXEL Device does not have an Ethernet connection with the WAN.
INTERNET	Green	On	The ZyXEL Device has an IP connection but no traffic. Your device has a WAN IP address (either static or assigned by a DHCP server), PPP negotiation was successfully completed (if used) and the DSL connection is up.
		Blinking	The ZyXEL Device is sending or receiving IP traffic.
	Red	On	The ZyXEL Device attempted to make an IP connection but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed.
		Off	The ZyXEL Device does not have an IP connection.
PHONE	Green	On	A SIP account is registered for the phone port.
		Blinking	A telephone connected to the phone port has its receiver off of the hook or there is an incoming call.
	Orange	On	A SIP account is registered for the phone port and there is a voice message in the corresponding SIP account.
		Blinking	A telephone connected to the phone port has its receiver off of the hook and there is a voice message in the corresponding SIP account.
		Off	The phone port does not have a SIP account registered.

Table 1 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
USB	Green/ Orange	On	The ZyXEL Device recognizes a USB connection but there is no traffic.
		Blinking	The ZyXEL Device is sending/receiving data to /from the USB device connected to it.
		Off	The ZyXEL Device does not detect a USB connection.

Refer to the Quick Start Guide for information on hardware connections.

1.6 The RESET Button

If you forget your password or cannot access the web configurator, you will need to use the **RESET** button at the back of the device to reload the factory-default configuration file. This means that you will lose all configurations that you had previously and the passwords will be reset to the defaults.

1 Make sure the **POWER** LED is on (not blinking).

2 To set the device back to the factory default settings, press the **RESET** button for ten seconds or until the **POWER** LED begins to blink and then release it. When the **POWER** LED begins to blink, the defaults have been restored and the device restarts.

1.7 The WPS/WLAN Button

Use the **WPS/WLAN** button ( ) on the top of the device to turn the wireless LAN off or on. You can also use it to activate WPS in order to quickly set up a wireless network with strong security. Make sure the **POWER** LED is on (not blinking) before using the **WLAN** button.

- Press the **WLAN** button for one second and release it. The **WLAN** LED should change from on to off or vice versa.
- Press the WLAN button for five seconds to turn on WPS. See Section 7.5 on page 143 for more on using WPS to configure your wireless clients.

2

Introducing the Web Configurator

2.1 Overview

The web configurator is an HTML-based management interface that allows easy device setup and management via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

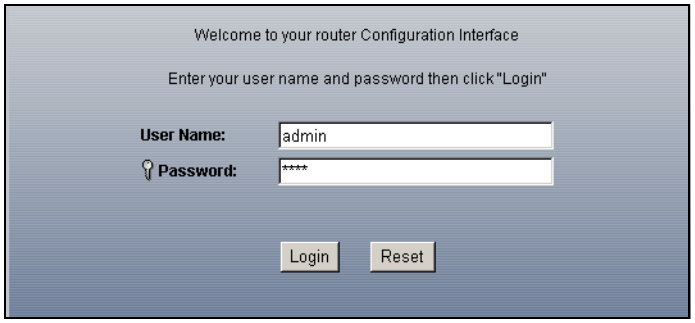
See Appendix C on page 335 if you need to make sure these functions are allowed in Internet Explorer.

2.1.1 Accessing the Web Configurator

1. Make sure your ZyXEL Device hardware is properly connected (refer to the Quick Start Guide).
2. Launch your web browser.
3. Type "192.168.1.1" as the URL.

4 A password screen displays. Type “admin” (default) as the username and “1234” as the password, and click **Login**. Click **Cancel** to revert to the default password in the password field. If you have changed the password, enter your password and click **Login**.

Figure 5 Password Screen

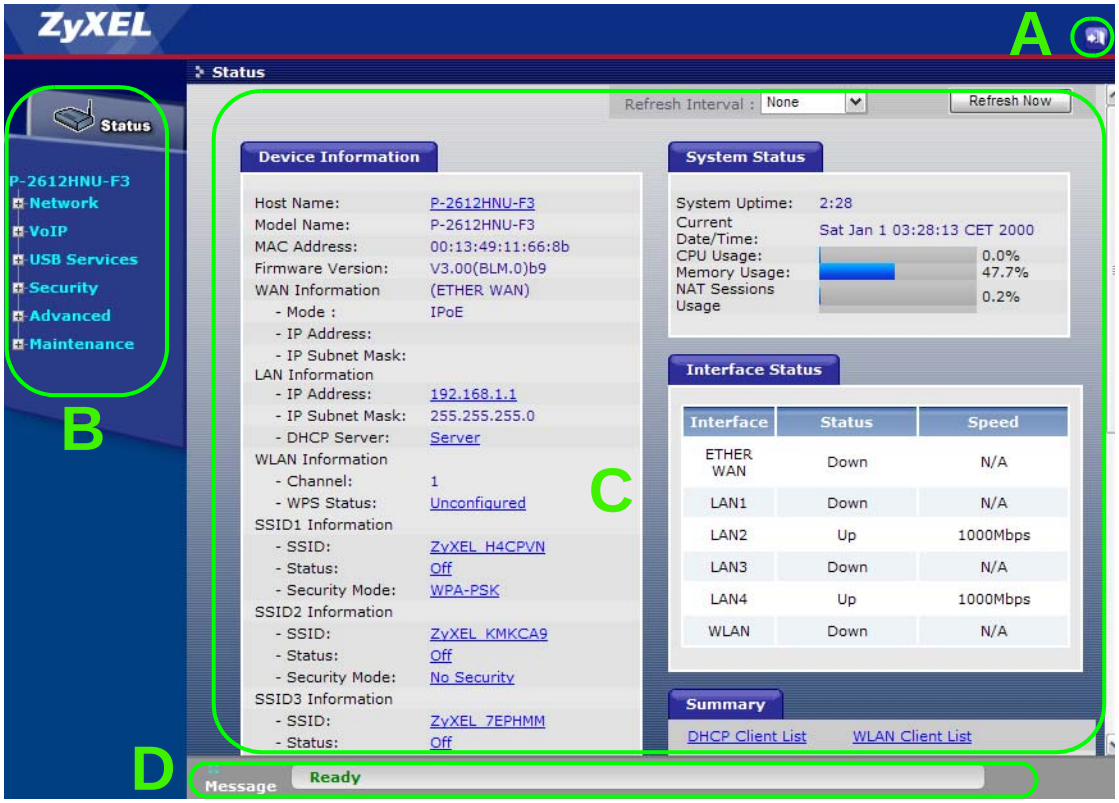


Note: For security reasons, the ZyXEL Device automatically logs you out if you do not use the web configurator for five minutes (default). If this happens, log in again.

2.2 Web Configurator Main Screen

The following screen shows after you have logged in.

Figure 6 Main Screen



As illustrated above, the main screen is divided into these parts:

- **A** - title bar
- **B** - navigation panel
- **C** - main window
- **D** - status bar

2.2.1 Title Bar

The title bar shows the following icon in the upper right corner.

Click this icon to log out of the web configurator.

2.2.2 Navigation Panel

Use the menu items on the navigation panel to open screens to configure ZyXEL Device features. The following table describes each menu item.

Table 2 Navigation Panel Summary

LINK	TAB	FUNCTION
Status		This screen shows the ZyXEL Device's general device and network status information. Use this screen to access the statistics and client list.
Network		
WAN	Layer 2 Interface	Use this screen to view, remove or add a layer-2 WAN interface.
	Internet Connection	Use this screen to configure ISP parameters, WAN IP address assignment, DNS servers and other advanced properties.
LAN	IP	Use this screen to configure LAN TCP/IP settings.
	DHCP Server	Use this screen to configure the DNS server information that the ZyXEL Device sends to the DHCP client devices on the LAN.
	Client List	Use this screen to view current DHCP client information and to always assign specific IP addresses to individual MAC addresses (and host names).

Table 2 Navigation Panel Summary

LINK	TAB	FUNCTION
Wireless LAN	General	Use this screen to turn the wireless connection on or off, specify the SSID(s) and make other configuration changes.
	Security	Use this screen to configure the wireless LAN settings and WLAN authentication/security settings.
	QoS	Use this screen to enable or disable wireless quality of service.
	WPS	Use this screen to use WPS (Wi-Fi Protected Setup) to establish a wireless connection.
	WPS Station	Use this screen to enable or disable WPS, generate a security PIN (Personal Identification Number) and see information about the ZyXEL Device's WPS status.
	Scheduling	Use this screen to configure when the ZyXEL Device enables or disables the wireless LAN.
	Association List	Use this screen to view wireless stations that are currently associated with the ZyXEL Device.
NAT	Port Forwarding	Use this screen to make your local servers visible to the outside world.
VoIP		
SIP	SIP Service Provider	Use this screen to configure your ZyXEL Device's Voice over IP settings.
	SIP Account	Use this screen to set up information about your SIP account, control which SIP accounts the phones connected to the ZyXEL Device use and configure audio settings such as volume levels for the phones connected to the ZyXEL Device.
Phone	Analog Phone	Use this screen to set which phone ports use which SIP accounts.
	Region	Use this screen to select your location and call service mode.
Phone Book	Speed Dial	Use this screen to configure speed dial for SIP phone numbers that you call often.
USB Services		
File Sharing	Share Configuration	Use this screen to enable file sharing server on the ZyXEL Device and configure the workgroup name.
	Account Management	Use this screen to set up and configure a file sharing account.
Media Server	Configuration	Use this screen to enable or disable the sharing of media files.
Print Server	Print Configuration	Use this screen to enable or disable sharing of a USB printer via your ZyXEL Device.
Security		
MAC Filter	MAC Filter	Use this screen to configure the ZyXEL Device to give exclusive access to specific wireless clients.

Table 2 Navigation Panel Summary

LINK	TAB	FUNCTION
Firewall	Services	Use this screen to activate/deactivate the firewall and set the default action to take on network traffic going in specific directions.
Certificates	My Certificates	Use this screen to generate and export self-signed certificates or certification requests and import the ZyXEL Device's CA-signed certificates.
	Trusted CAs	Use this screen to save CA certificates to the ZyXEL Device.
Advanced		
Static Route	Static Route	Use this screen to configure IP static routes to tell your device about networks beyond the directly connected remote nodes.
QoS	General	Use this screen to enable QoS and decide allowable bandwidth using QoS.
	Queue Setup	Use this screen to configure QoS queue assignment.
	Class Setup	Use this screen to set up classifiers to sort traffic into different flows and assign priority and define actions to be performed for a classified traffic flow.
	Monitor	Use this screen to view each queue's statistics.
Dynamic DNS	Dynamic DNS	This screen allows you to use a static hostname alias for a dynamic IP address.
Service Control	Service Control	Use this screen to configure through which interface(s) users can use which service(s) to manage the ZyXEL Device.
Maintenance		
System	General	Use this screen to configure your device's name, domain name, management inactivity timeout and password.
	Time Setting	Use this screen to change your ZyXEL Device's time and date.
Logs	View Log	Use this screen to display your device's logs.
	Log Settings	Use this screen to select which logs and/or immediate alerts your device is to record. You can also set it to e-mail the logs to you.
Tools	Firmware	Use this screen to upload firmware to your device.
	Configuration	Use this screen to backup and restore your device's configuration (settings) or reset the factory default settings.
	Restart	This screen allows you to reboot the ZyXEL Device without turning the power off.
Diagnostic	DSL Line	Use this screen to test the connections to other devices.

Table 2 Navigation Panel Summary

LINK	TAB	FUNCTION
Account	Admin	Use this screen to change the password for the Administrator account for your ZyXEL Device.
	User	Use this screen to change the password for the User account for your ZyXEL Device.

2.2.3 Main Window

The main window displays information and configuration fields. It is discussed in the rest of this document.

Right after you log in, the **Status** screen is displayed. See Chapter 4 on page 85 for more information about the **Status** screen.

2.2.4 Status Bar

Check the status bar when you click **Apply** or **OK** to verify that the configuration has been updated.

3

Tutorial

3.1 Overview

This chapter contains the following tutorials:

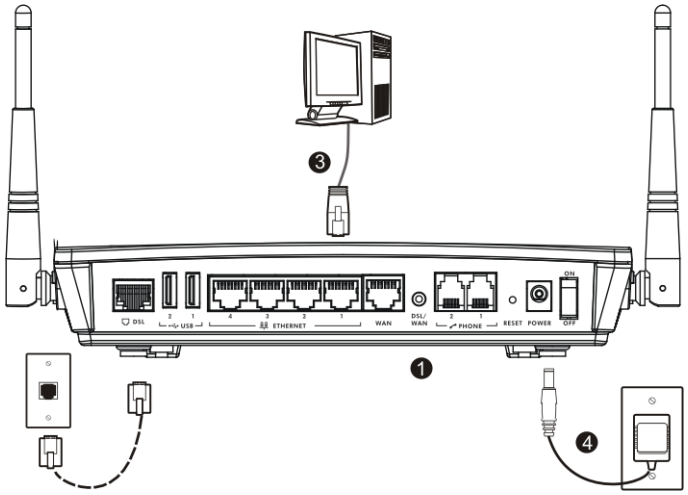
- Setting Up Your DSL Connection
- How to Set up a Wireless Network
- Setting Up NAT Port Forwarding
- How to Make a VoIP Call
- Using the File Sharing Feature
- Using the Media Server Feature
- Using the Print Server Feature
- Configuring the MAC Address Filter
- Configuring Static Route for Routing to Another Network
- Configuring QoS Queue and Class Setup
- Access the ZyXEL Device Using DDNS

3.2 Setting Up Your DSL Connection

This tutorial shows you how to set up your Internet connection using the Web Configurator.

If you connect to the Internet through a DSL connection, use the information from your Internet Service Provider (ISP) to configure the ZyXEL Device. Do the following steps:

Hardware Preparation



1 Check the back panel of your device where the Ethernet ports are located and make sure the **DSL/WAN** switch is pointing up.

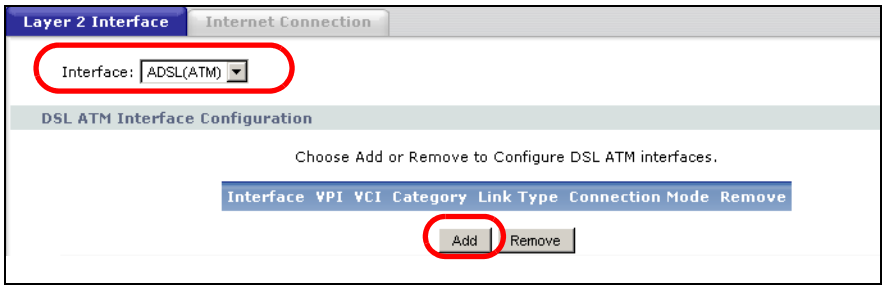
2 Connect one end of an Ethernet cable to the DSL port of your ZyXEL Device. The other end should be connected to the DSL port in your house or a DSL router/ modem provided by your ISP.

3 Connect one end of another Ethernet cable to an Ethernet port on the ZyXEL Device and the other end to a computer that you will use to access the Web Configurator.

4 Connect the ZyXEL Device to a power source, turn it on and wait for the POWER LED to become a steady green. Turn on the modem provided by your ISP as well as the computer.

Account Configuration

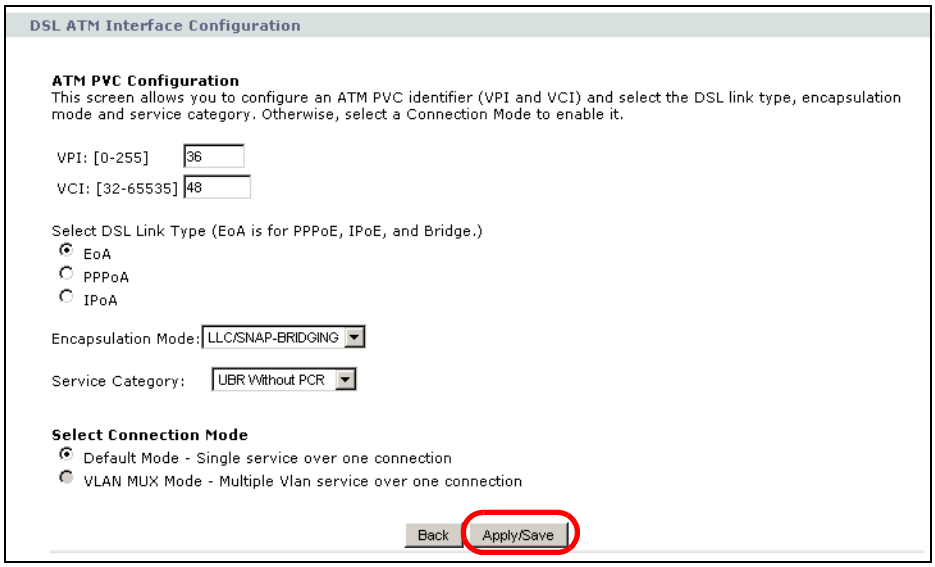
1 Click **Network > WAN > Layer 2 Interface** to open the following screen. Select **DSL (ATM)** as the **Interface** and click **Add**.



2 For this example, the DSL connection has the following information.

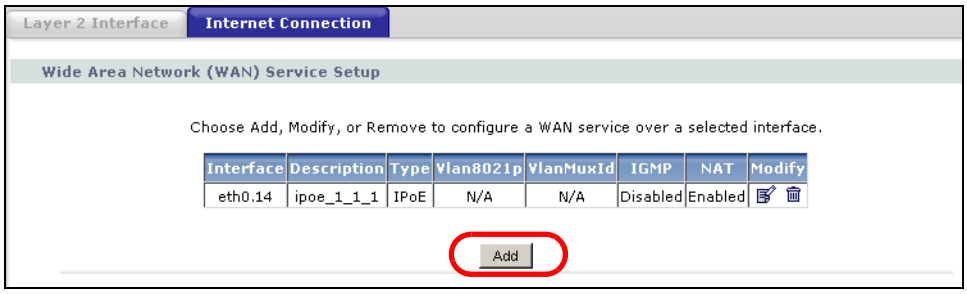
VPI / VCI	36/48
DSL Link Type	EoA
Encapsulation Mode	LLC/SNAP-Bridging
Service Category	UBR without PCR
Select Connection Mode	Default Mode

Enter or select these values and click **Apply / Save**.

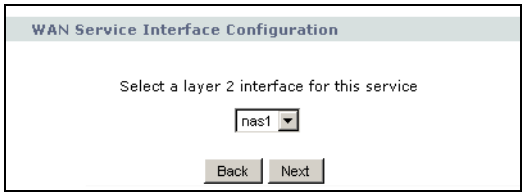

DSL ATM Interface Configuration
ATM PVC Configuration
This screen allows you to configure an ATM PVC identifier (VPI and VCI) and select the DSL link type, encapsulation mode and service category. Otherwise, select a Connection Mode to enable it.
VPI: [0-255] 36
VCI: [32-65535] 48
Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)
EoA
PPPoA
IPoA
Encapsulation Mode: LLC/SNAP-BRIDGING
Service Category: UBR Without PCR
Select Connection Mode
Default Mode - Single service over one connection
VLAN MUX Mode - Multiple Vlan service over one connection
Back
Apply/Save

This creates your layer-2 ATM interface.

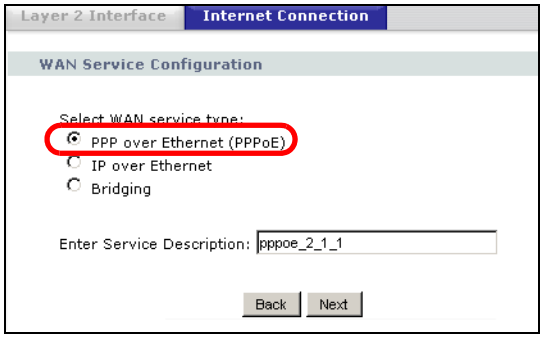
3 Click **WAN > Internet Connection** to open the following screen. Click **Add** to enter your DSL connection details.


Layer 2 Interface
Internet Connection
Wide Area Network (WAN) Service Setup
Choose Add, Modify, or Remove to configure a WAN service over a selected interface.
Interface Description Type Vlan8021p VlanMuxId IGMP NAT Modify
eth0.14 ipoe_1_1_1 IPoE N/A N/A Disabled Enabled
Add

4 Select **nas1** as your layer 2 interface and click **Next**. This is the interface you created in the **WAN > Layer 2 Interface** screen.

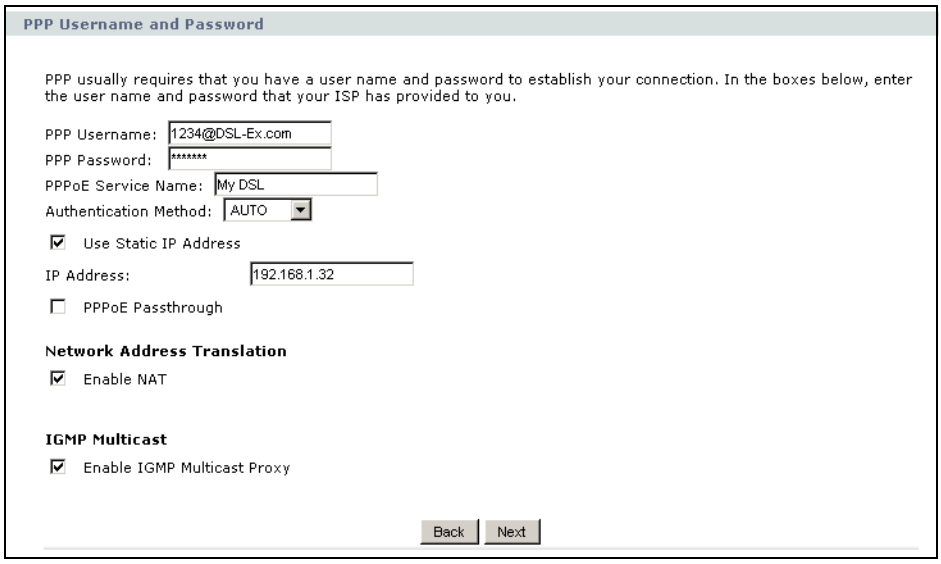


5 Choose the **WAN Service Type** specified by your DSL service provider. For this example, the service provider requires a username and password to establish Internet connection. Therefore, select **PPPoE** as the WAN service type and click **Next**. You can also enter a brief description for this service or user the default name given by the ZyXEL Device, which is **pppoe_2_1_1** in this example.



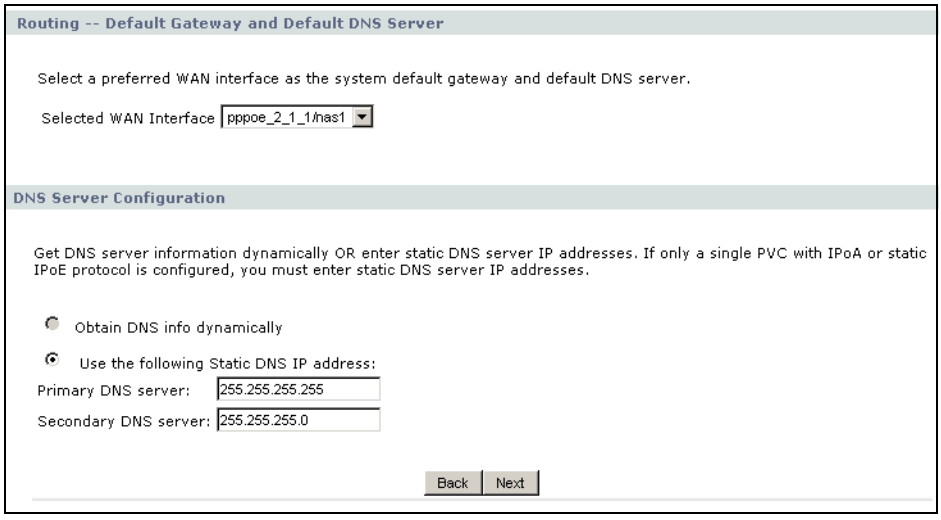
6 In the following screen, enter the account information provided to you. The following values are used here:

PPP Username	1234@DSL-Ex.com
PPP Password	ABCDEF!
PPPoE Service Name	My DSL
Authentication Method	AUTO
Static IP Address	192.168.1.32
Others	PPPoE Passthrough: Disabled NAT: Enabled IGMP Multicast Proxy: Enabled

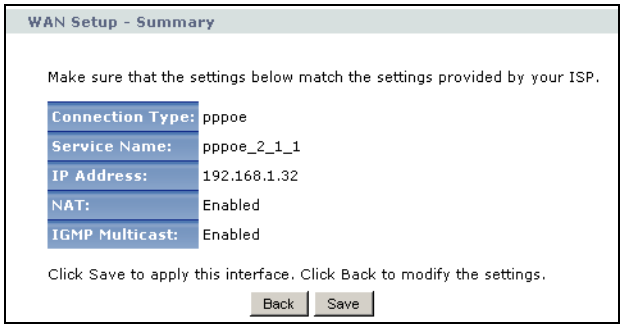

PPP Username and Password
PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.
PPP Username: 1234@DSL-Ex.com
PPP Password: *******
PPPoE Service Name: My DSL
Authentication Method: AUTO
Use Static IP Address
IP Address: 192.168.1.32
PPPoE Passthrough
Network Address Translation
Enable NAT
IGMP Multicast
Enable IGMP Multicast Proxy
Back
Next

Click **Next**.

7 In the following screen, select **pppoe_2_1_1/nas1** as your default Internet connection. And enter the DNS server addresses provided to you, such as **255.255.255.0** (primary)/**255.255.254.0** (secondary). Click **Next**.


Routing -- Default Gateway and Default DNS Server
Select a preferred WAN interface as the system default gateway and default DNS server.
Selected WAN Interface pppoe_2_1_1/nas1
DNS Server Configuration
Get DNS server information dynamically OR enter static DNS server IP addresses. If only a single PVC with IPoA or static IPoE protocol is configured, you must enter static DNS server IP addresses.
Obtain DNS info dynamically
Use the following Static DNS IP address:
Primary DNS server: 255.255.255.255
Secondary DNS server: 255.255.255.0
Back
Next

8 You should see a summary of your DSL setup as follows.


WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
Connection Type: pppoe
Service Name: pppoe_2_1_1
IP Address: 192.168.1.32
NAT: Enabled
IGMP Multicast: Enabled
Click Save to apply this interface. Click Back to modify the settings.
Back
Save

Click **Save** to start using your settings. Try to connect to a website, such as zyxel.com to see if you have correctly set up your Internet connection. Be sure to contact your service provider for any information you need to configure the WAN screens.

3.3 How to Set up a Wireless Network

This section gives you examples of how to set up an access point and wireless client for wireless communication using the following parameters. The wireless clients can access the Internet through the ZyXEL Device wirelessly.

3.3.1 Example Parameters

SSID	SSID_Example3
Security	WPA-PSK (Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey)
802.11 mode	802.11b/g

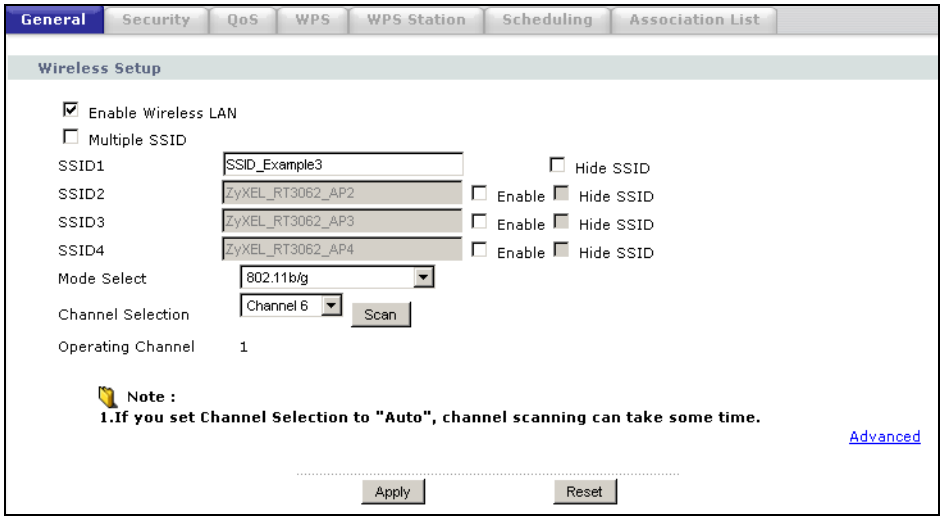
An access point (AP) or wireless router is referred to as the “AP” and a computer with a wireless network card or USB adapter is referred to as the “wireless client” here.

The M-302 utility screens are used here as an example. The screens may vary slightly for different models.

3.3.2 Configuring the AP

Follow the steps below to configure the wireless settings on your AP.

1 Open the **Network > Wireless LAN > General** screen in the AP's web configurator.

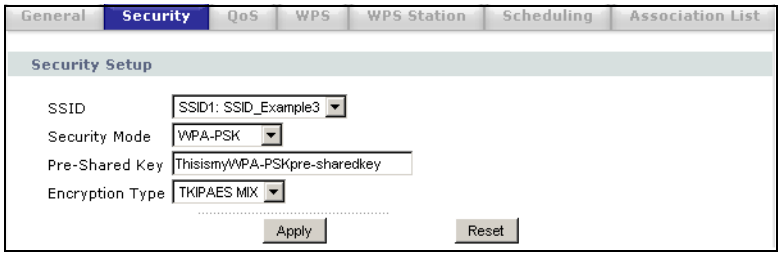


2 Make sure **Active Wireless LAN** is selected.

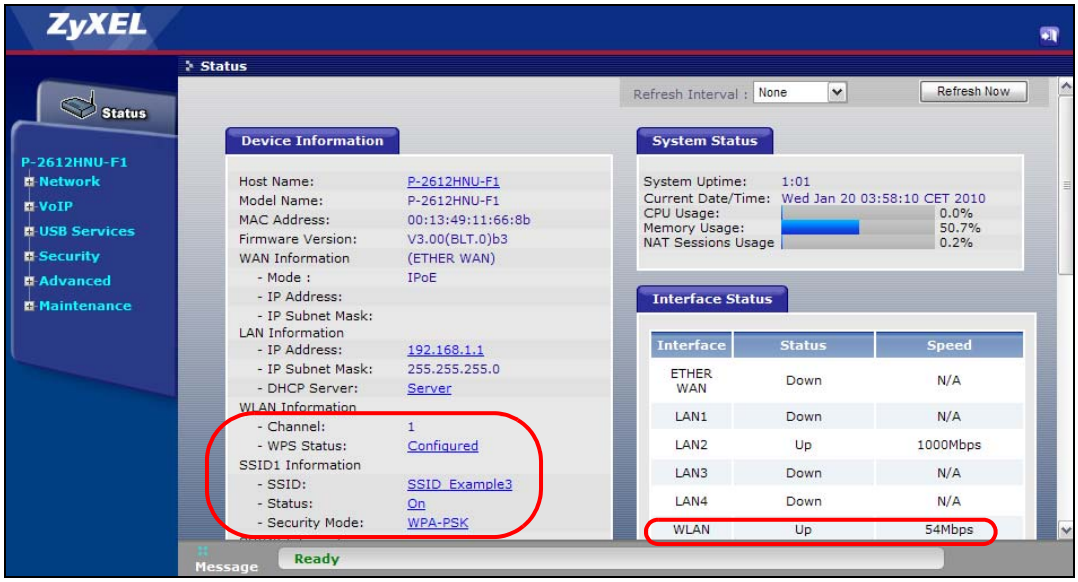
3 Enter "SSID_Example3" as the SSID and select a channel which is not used by another AP.

4 Select **802.11b/g** in the **Mode Select** field. Click **Apply**.

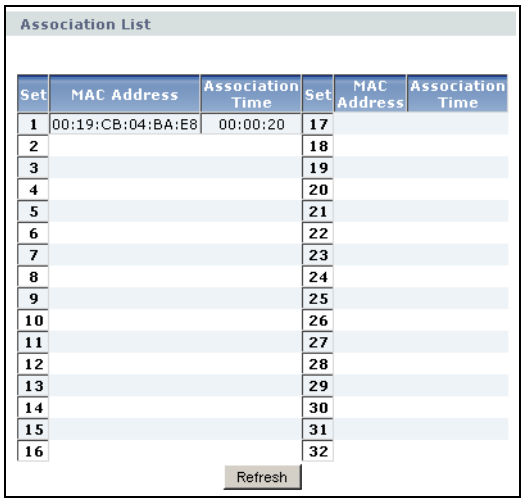
5 Open **Network > Wireless LAN > Security**. Set security mode to **WPA-PSK** and enter "ThisismyWPA-PSKpre-sharedkey" in the **Pre-Shared Key** field. Click **Apply**.



6 Open the **Status** screen. Verify your wireless and wireless security settings under **Device Information** and check if the WLAN connection is up under **Interface Status**.



7 Click the **WLAN Client List** hyperlink in the AP's **Status** screen. You can see if any wireless client has connected to the AP.

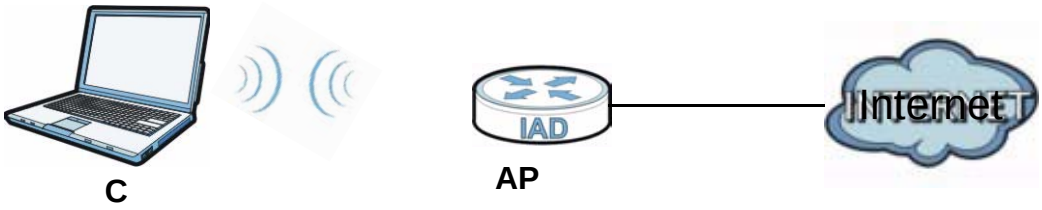


3.3.3 Configuring the Wireless Client

This section describes how to connect the wireless client to a network.

3.3.3.1 Connecting to a Wireless LAN

The following sections show you how to join a wireless network using the ZyXEL utility, as in the following diagram. The wireless client is labeled **C** and the access point is labeled **AP**.



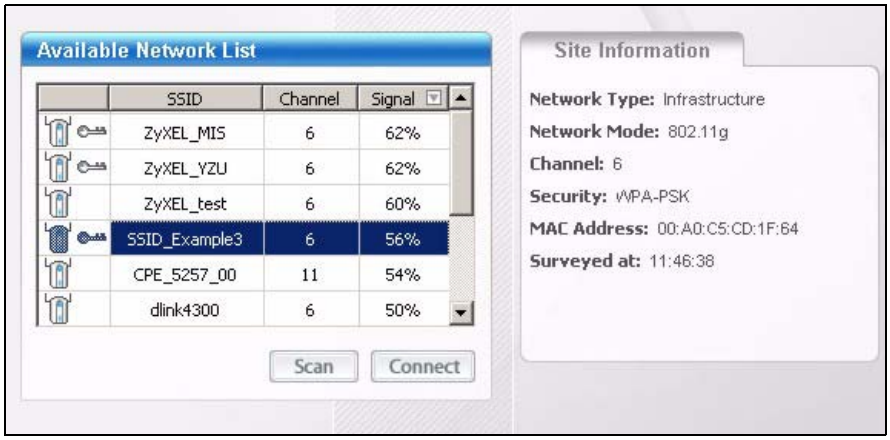
There are three ways to connect the client to an access point.

- Configure nothing and leave the wireless client to automatically scan for and connect to any available network that has no wireless security configured.
- Manually connect to a network.
- Configure a profile to have the wireless client automatically connect to a specific network or peer computer.

This example illustrates how to manually connect your wireless client to an access point (AP) which is configured for WPA-PSK security and connected to the Internet. Before you connect to the access point, you must know its Service Set IDentity (SSID) and WPA-PSK pre-shared key. In this example, the SSID is “SSID_Example3” and the pre-shared key is “ThisismyWPA-PSKpre-sharedkey”.

After you install the ZyXEL utility and then insert the wireless client, follow the steps below to connect to a network using the **Site Survey** screen.

1 Open the ZyXEL utility and click the **Site Survey** tab to open the screen shown next.

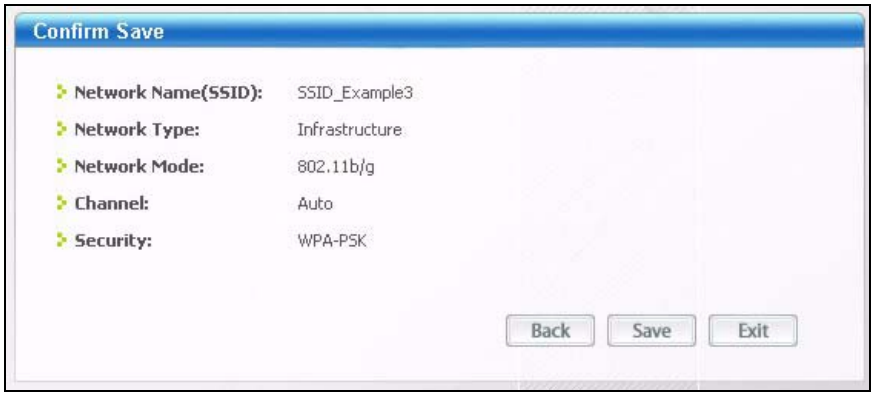


2 The wireless client automatically searches for available wireless networks. Click **Scan** if you want to search again. If no entry displays in the **Available Network List**, that means there is no wireless network available within range. Make sure the AP or peer computer is turned on or move the wireless client closer to the AP or peer computer.

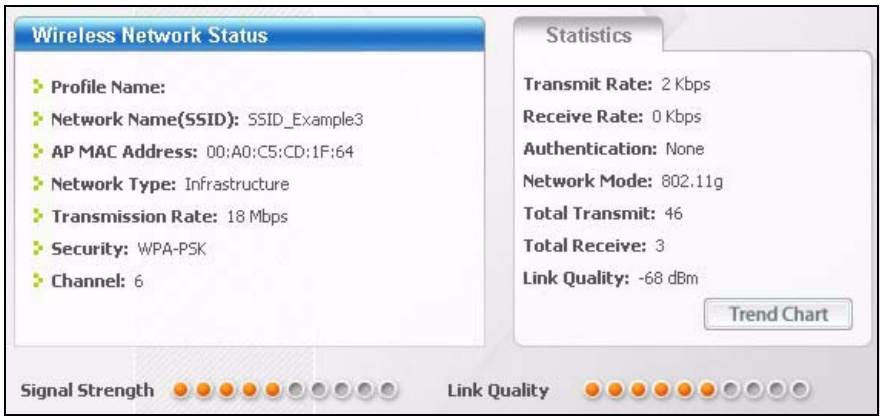
3 When you try to connect to an AP with security configured, a window will pop up prompting you to specify the security settings. Enter the pre-shared key and leave the encryption type at the default setting.

Use the **Next** button to move on to the next screen. You can use the **Back** button at any time to return to the previous screen, or the **Exit** button to return to the **Site Survey** screen.

4 The **Confirm Save** window appears. Check your settings and click **Save** to continue.



5 The ZyXEL utility returns to the **Link Info** screen while it connects to the wireless network using your settings. When the wireless link is established, the ZyXEL utility icon in the system tray turns green and the **Link Info** screen displays details of the active connection. Check the network information in the **Link Info** screen to verify that you have successfully connected to the selected network. If the wireless client is not connected to a network, the fields in this screen remain blank.



6 Open your Internet browser and enter http://www.zyxel.com or the URL of any other web site in the address bar. If you are able to access the web site, your wireless connection is successfully configured.

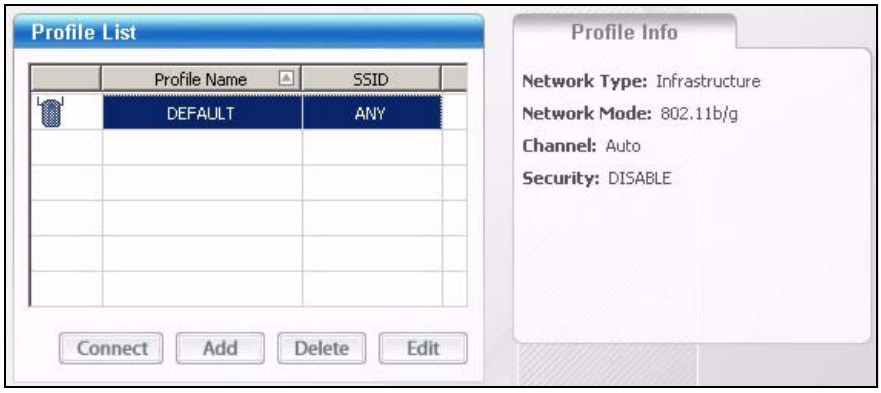
If you cannot access the web site, try changing the encryption type in the **Security Settings** screen, check the Troubleshooting section of this User's Guide or contact your network administrator.

3.3.3.2 Creating and Using a Profile

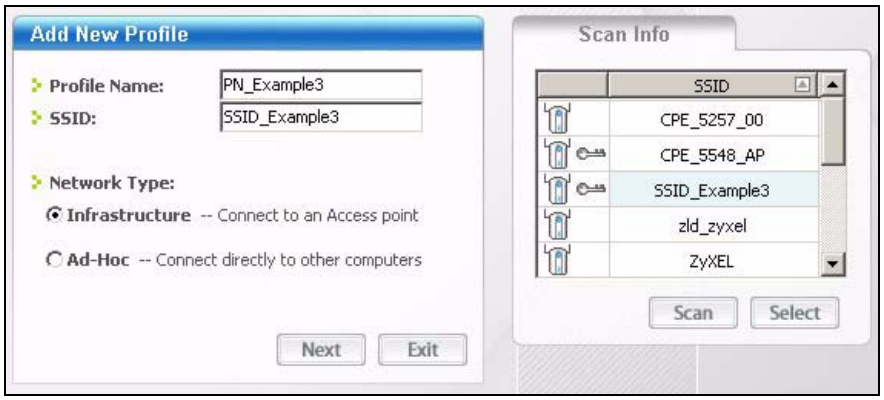
A profile lets you easily connect to the same wireless network again later. You can also configure different profiles for different networks, for example if you connect a notebook computer to wireless networks at home and at work.

This example illustrates how to set up a profile and connect the wireless client to an AP configured for WPA-PSK security. In this example, the SSID is “SSID_Example3”, the profile name is “PN_Example3” and the pre-shared key is “ThisismyWPA-PSKpre-sharedkey”. You have chosen the profile name “PN_Example3”.

1 Open the ZyXEL utility and click the **Profile** tab to open the screen shown next. Click **Add** to configure a new profile.



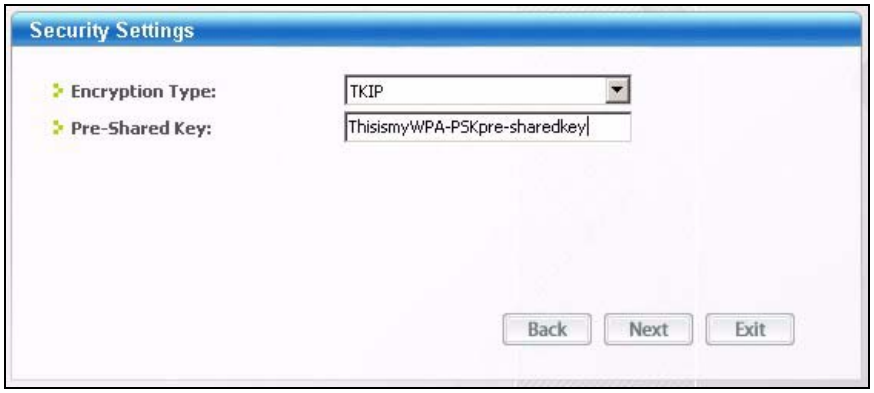
2 The **Add New Profile** screen appears. The wireless client automatically searches for available wireless networks, and displays them in the **Scan Info** box. Click **Scan** if you want to search again. You can also configure your profile for a wireless network that is not in the list.



3 Give the profile a descriptive name (of up to 32 printable ASCII characters). Select **Infrastructure** and either manually enter or select the AP's SSID in the **Scan Info** table and click **Select**.

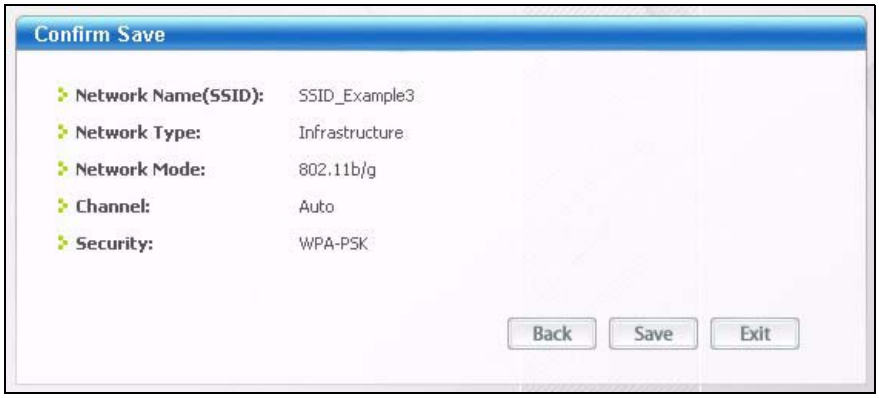
4 Choose the same encryption method as the AP to which you want to connect (In this example, WPA-PSK).

5 This screen varies depending on the encryption method you selected in the previous screen. Enter the pre-shared key and leave the encryption type at the default setting.



6 In the next screen, leave both boxes selected.

7 Verify the profile settings in the read-only screen. Click **Save** to save and go to the next screen.



8 Click **Activate Now** to use the new profile immediately. Otherwise, click the **Activate Later** button.

If you clicked **Activate Later**, you can select the profile from the list in the **Profile** screen and click **Connect** to activate it.

Note: Only one profile can be activated and used at any given time.

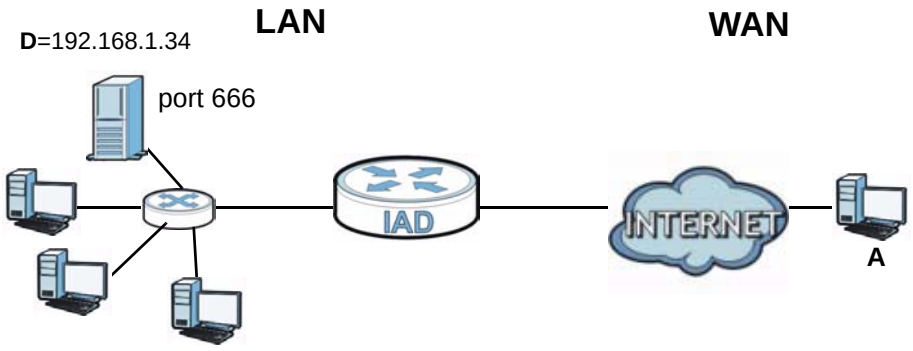
9 When you activate the new profile, the ZyXEL utility returns to the **Link Info** screen while it connects to the AP using your settings. When the wireless link is established, the ZyXEL utility icon in the system tray turns green and the **Link Info** screen displays details of the active connection.

10 Open your Internet browser, enter http://www.zyxel.com or the URL of any other web site in the address bar and press ENTER. If you are able to access the web site, your new profile is successfully configured.

11 If you cannot access the Internet go back to the **Profile** screen, select the profile you are using and click **Edit**. Check the details you entered previously. Also, refer to the Troubleshooting section of this User's Guide or contact your network administrator if necessary.

3.4 Setting Up NAT Port Forwarding

Thomas manages the Doom server on a computer behind the ZyXEL Device. In order for players on the Internet (like **A** in the figure below) to communicate with the Doom server, Thomas needs to configure the port settings and IP address on the ZyXEL Device. Traffic should be forwarded to the port 666 of the Doom server computer which has an IP address of 192.168.1.34.

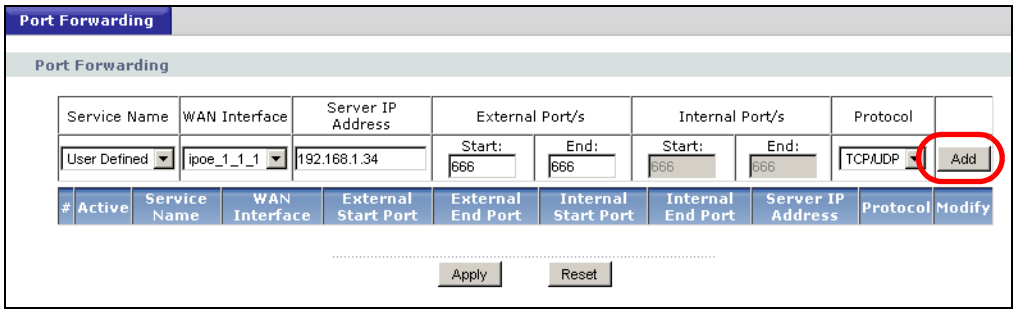


Thomas may set up the port settings by configuring the port settings for the Doom server computer (see Section 8.1.2 on page 149 for more information).

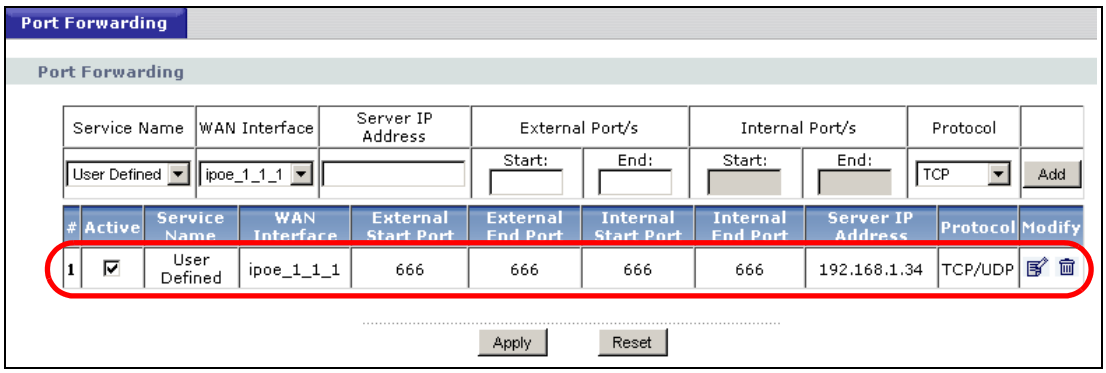
1 Click **Network** > **NAT** to open the **Port Forwarding** screen. Enter the following values:

Service Name	Select **User Defined**.
WAN Interface	Select the WAN interface through which the Doom service is forwarded. This is the default interface for this example, which is **ipoe_1_1_1**.
Server IP Address	Enter the IP address of the Doom server. This is **192.168.1.34** for this example.
External Port/s	Enter **666** as the **Start** and **End** port.
Protocol	Select **TCP/UDP**. This should be the protocol supported by the Doom server.

2 The screen should display as follows. Click **Add**.



3 The port forwarding settings you configured should appear in the table. Click **Apply** to have the ZyXEL Device start forwarding port 666 traffic to the computer with IP address 192.168.1.34.



Players on the Internet then can have access to Thomas' Doom server.

3.5 How to Make a VoIP Call

You can register a SIP account with the SIP server and make voice calls over the Internet to another VoIP device.

3.5.1 VoIP Calls With a Registered SIP Account

To use a registered SIP account, you should have applied for a SIP account with the VoIP service provider.

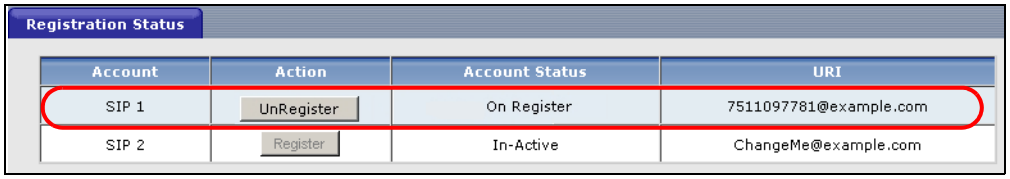
3.5.1.1 SIP Account Registration

Follow the steps below to register and activate your SIP account.

1 Make sure your ZyXEL Device is connected to the Internet.

2 Open the web configurator.

3 Go to the **Status** screen to check if your SIP account has been registered successfully. If registration failed, check your Internet connection and click **Register** to register your SIP account again.



3.5.1.2 Analog Phone Configuration

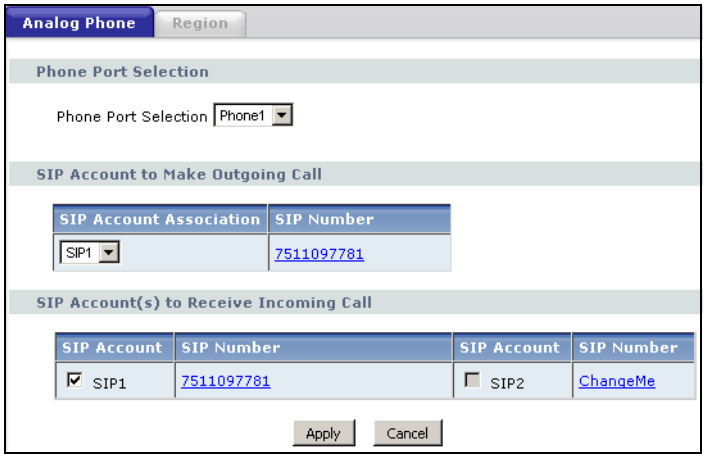
1 Click **VoIP > Phone** to open the **Analog Phone** screen.

2 Select **Phone1** to configure the first phone port.

3 Select **SIP1** from the **SIP Account** drop-down list box in the **SIP Account to Make Outgoing Call** section to have the phone (connected to the first phone port) use the registered SIP1 account to make outgoing calls.

4 Select the **SIP1** check box in the **SIP Account(s) to Receive Incoming Call** section to have the phone (connected to the first phone port) receive phone calls for the SIP1 account.

5 Click **Apply** to save your changes.



3.5.1.3 Making a VoIP Call

1 Make sure you connect a telephone to the first phone port on the ZyXEL Device.

2 Make sure the ZyXEL Device is on and connected to the Internet.

3 Pick up the phone receiver.

4 Dial the VoIP phone number you want to call.

3.6 Using the File Sharing Feature

In this section you can:

- Set up file sharing
- Access the shared files from a computer

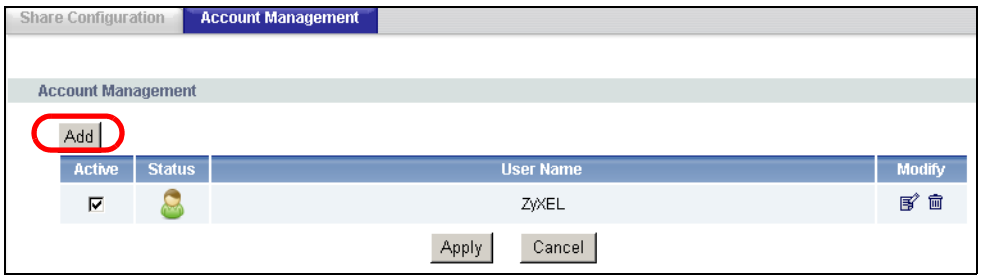
3.6.1 Set Up File Sharing

To set up file sharing you need to set up a user account, enable file sharing and set up your share(s).

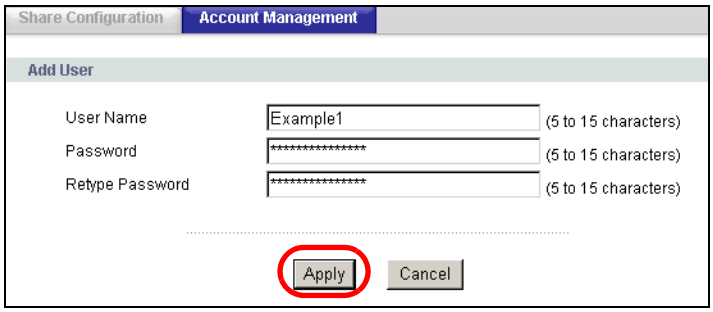
3.6.1.1 Set up a User Account

Before you can share files you need a user account.

1 Click **USB Services > File Sharing > Account Management** to display the following screen. Click **Add** to set up a user name and password.



2 The following screen appears. Enter a user name and password as shown in the example screen below. Click **Apply** to save your settings.

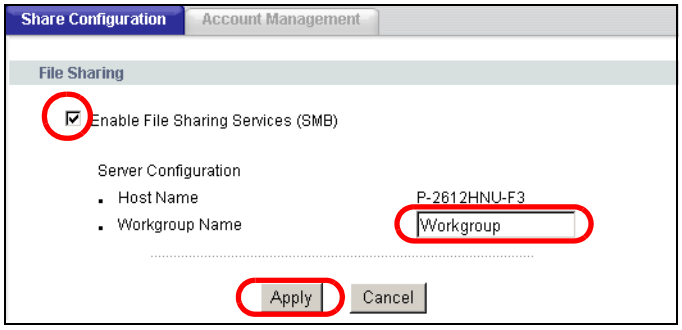


3 This sets up your user account, now you are ready to set up file sharing on your ZyXEL Device.

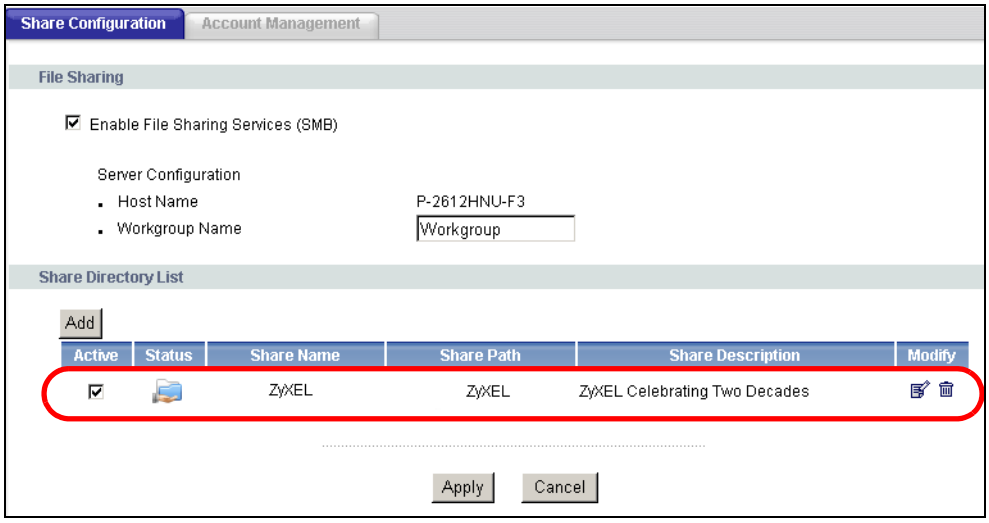
3.6.1.2 Set up File Sharing on Your ZyXEL Device

You also need to set up file sharing on your ZyXEL Device in order to share files.

1 Go to **USB Services > File Sharing > Share Configuration** to enable file sharing and enter a workgroup name. Click **Apply** to save your settings.



2 This sets up the file sharing server. You can see the USB storage device listed in the table below.



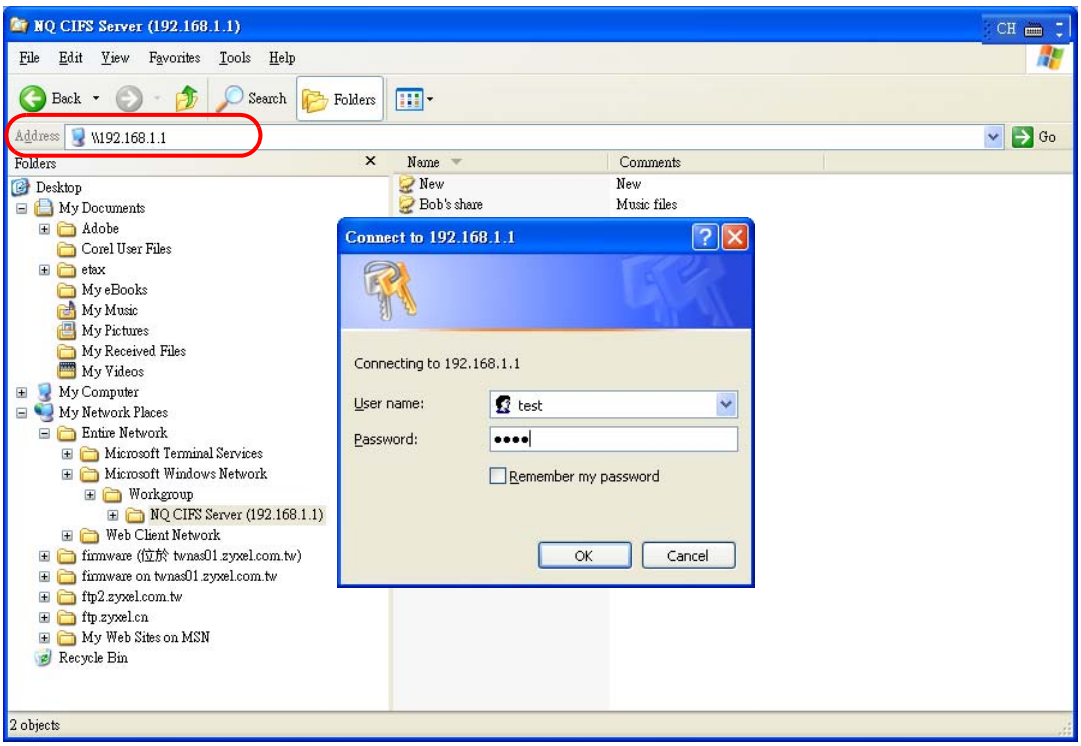
3.6.2 Access Your Shared Files From a Computer

You can use Windows Explorer to access the file storage devices connected to the ZyXEL Device.

Note: The examples in this User's Guide show you how to use Microsoft's Windows XP to browse your shared files. Refer to your operating system's documentation for how to browse your file structure.

Open Windows Explorer to access Bob's Share using Windows Explorer browser.

1 In Windows Explorer's Address bar type a double backslash "\\" followed by the IP address of the ZyXEL Device (the default IP address of the ZyXEL Device is 192.168.1.1) and press [ENTER]. A screen asking for password authentication appears. Type the user name and password and click **OK**.



Once you login to the file "Bob's Share" via your ZyXEL Device, you do not have to relogin unless you restart your computer.

3.7 Using the Media Server Feature

Use the media server feature to play files on a computer or on your television (using DMA-2500).

This section shows you how the media server feature works using the following media clients:

- Microsoft (MS) Windows Media Player

  Media Server works with Windows Vista and Windows 7. Make sure your computer is able to play media files (music, videos and pictures).

- ZyXEL DMA-2500, a digital media adapter

  You need to set up the DMA-2500 to work with your television (TV). Refer to the DMA-2500 Quick Start Guide for the correct hardware connections.

Before you begin, connect the USB storage device containing the media files you want to play to the USB port of your ZyXEL Device.

3.7.1 Configuring the ZyXEL Device

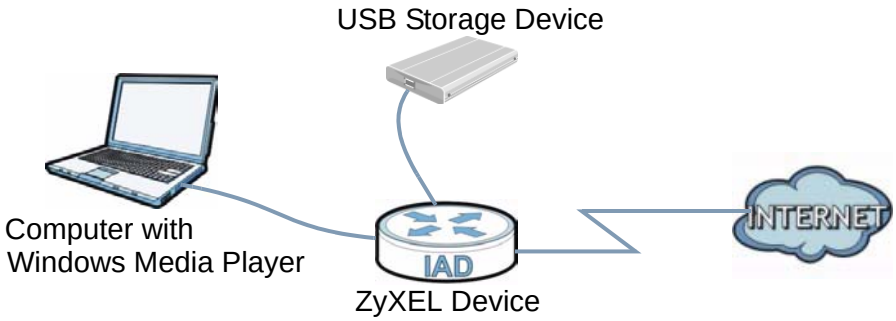
Note: The Media Server feature is enabled by default.

To use your ZyXEL Device as a media server, click **USB Services > Media Server.**

Check **Enable Media Server** and click **Apply**. This enables DLNA-compliant media clients to play the video, music and image files in your USB storage device.

3.7.2 Using Windows Media Player

This section shows you how to play the media files on the USB storage device connected to your ZyXEL Device using Windows Media Player.



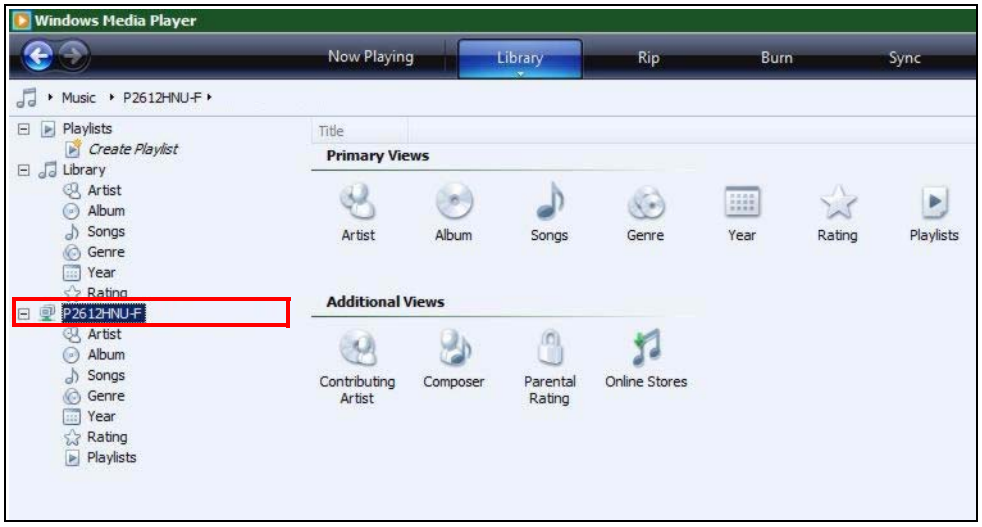
Windows Vista

1 Open Windows Media Player and click **Library > Media Sharing** as follows.

2 Check **Find media that others are sharing** in the following screen and click **OK**.

Media Sharing
Find and share music, pictures, and video on your network
Learn about sharing Online
Sharing settings
Find media that others are sharing
Share my media
Your network (Network) is a private network. Devices that you allow can find your shared media.
Networking...
How does sharing change firewall settings?
OK
Cancel

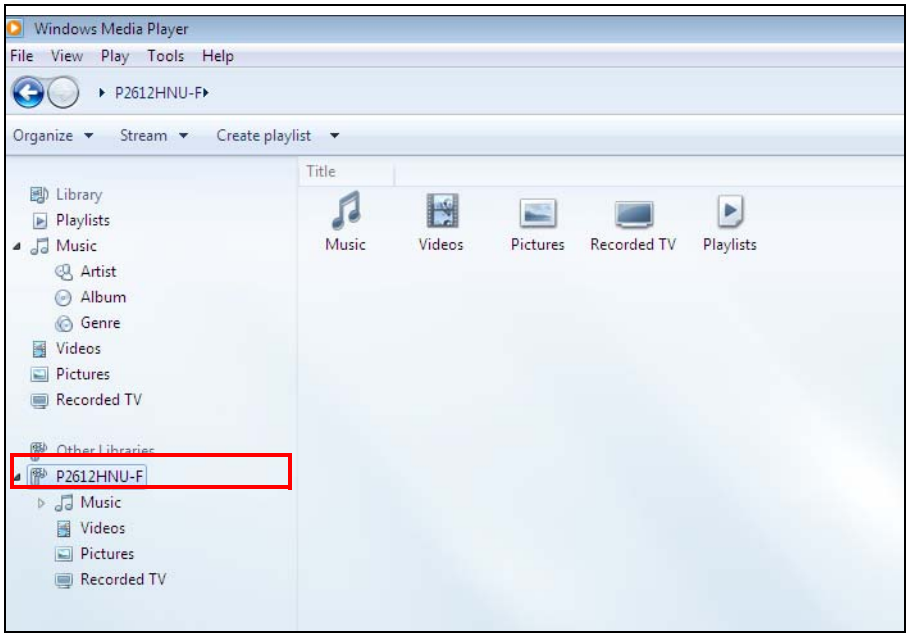
3 In the **Library** screen, check the left panel. The Windows Media Player should detect the ZyXEL Device.



The ZyXEL Device displays as a playlist. Clicking on the category icons in the right panel shows you the media files in the USB storage device attached to your ZyXEL Device.

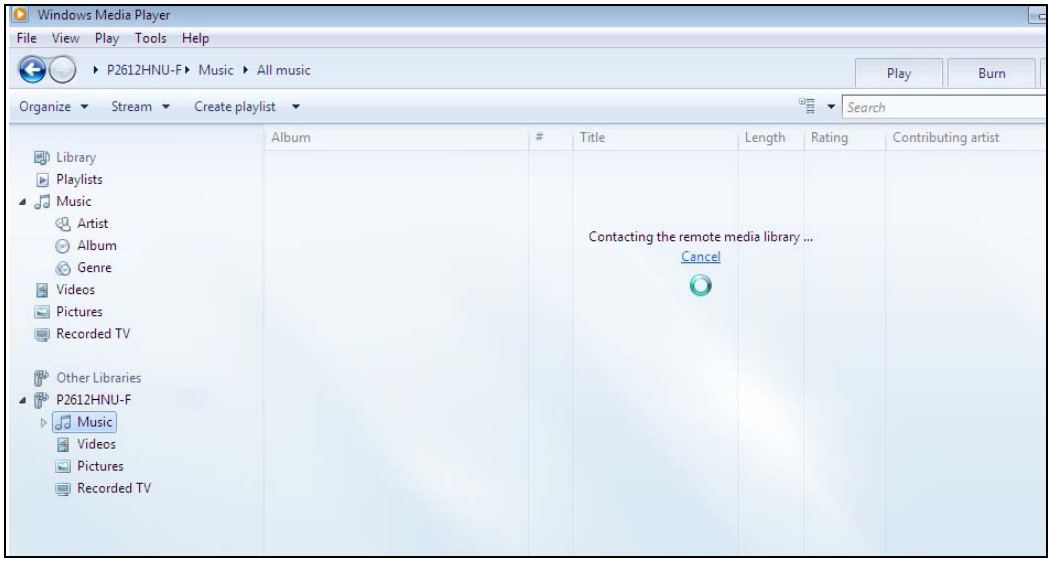
Windows 7

1 Open Windows Media Player. It should automatically detect the ZyXEL Device.

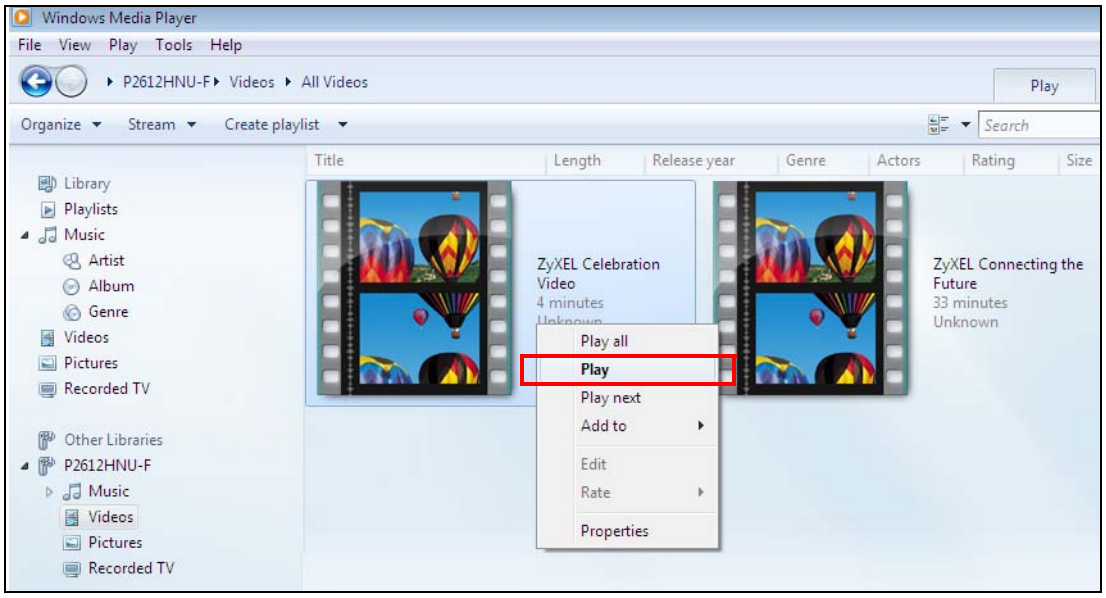


If you cannot see the ZyXEL Device in the left panel as shown above, right-click **Other Libraries > Refresh Other Libraries**.

2 Select a category in the left panel and wait for Windows Media Player to connect to the ZyXEL Device.



3 In the right panel, you should see a list of files available in the USB storage device.

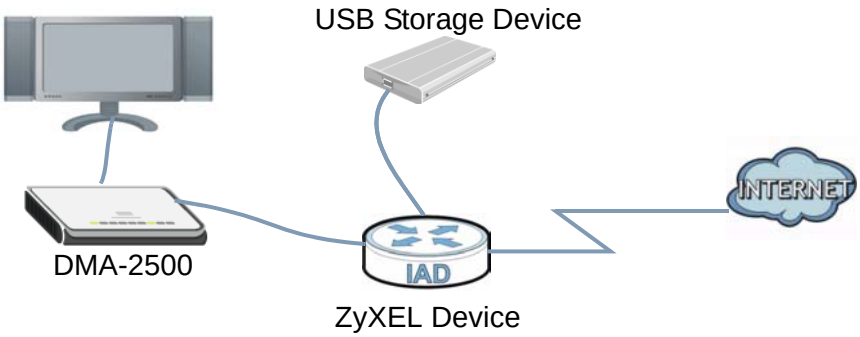


3.7.3 Using a Digital Media Adapter

This section shows you how you can use the ZyXEL Device with a ZyXEL DMA-2500 to play media files stored in the USB storage device in your TV screen.

Note: For this tutorial, your DMA-2500 should already be set up with the TV according to the instructions in the DMA-2500 Quick Start Guide.

1 Connect the DMA-2500 to an available LAN port in your ZyXEL Device.



2 Turn on the TV and wait for the DMA-2500 **Home** screen to appear. Using the remote control, go to **MyMedia** to open the following screen. Select the ZyXEL Device as your media server.

3 The screen shows you the list of available media files in the USB storage device. Select the file you want to open and push the **Play** button in the remote control.

3.8 Using the Print Server Feature

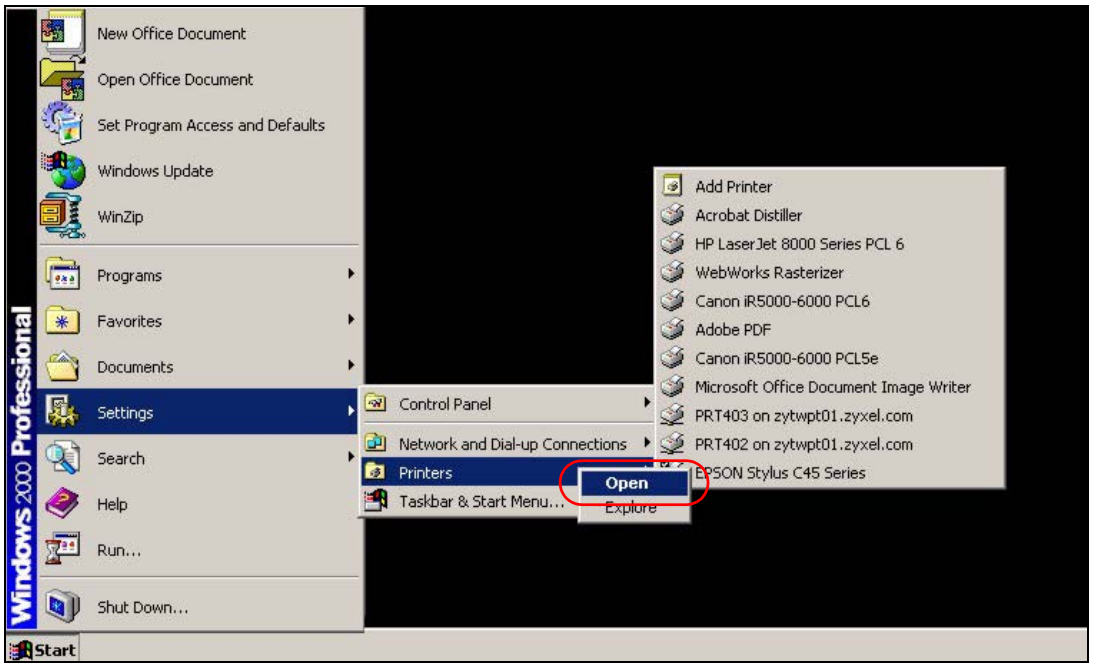
In this section you can:

- Configure a TCP/IP Printer Port
- Add a New Printer Using Windows
- Add a New Printer Using Macintosh OS X

Configure a TCP/IP Printer Port

This example shows how you can configure a TCP/IP printer port. This example is done using the Windows 2000 Professional operating system. Some menu items may look different on your operating system. The TCP/IP port must be configured with the IP address of the ZyXEL Device and must use the LPR protocol to communicate with the printer. Consult your operating systems documentation for instructions on how to do this or follow the instructions below if you have a Windows 2000/XP operating system.

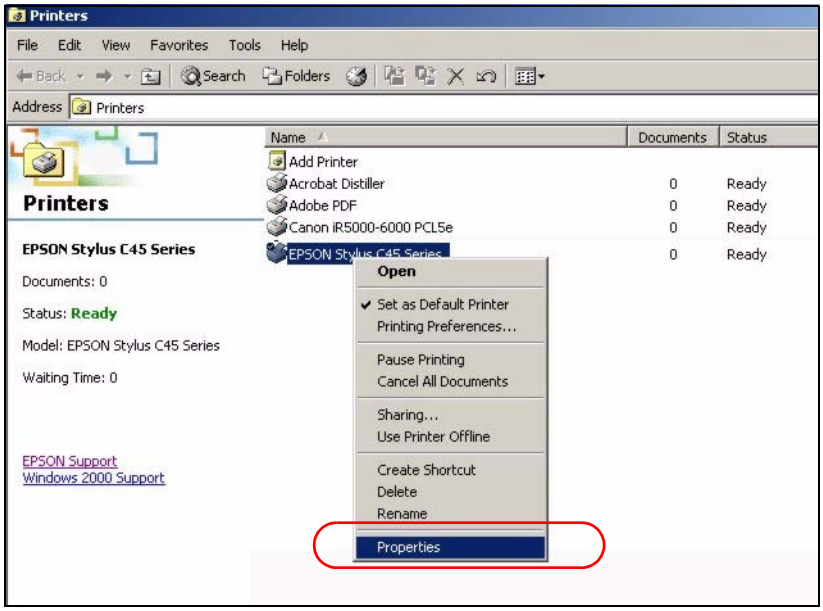
1 Click **Start** > **Settings**, then right click on **Printers** and select **Open**.



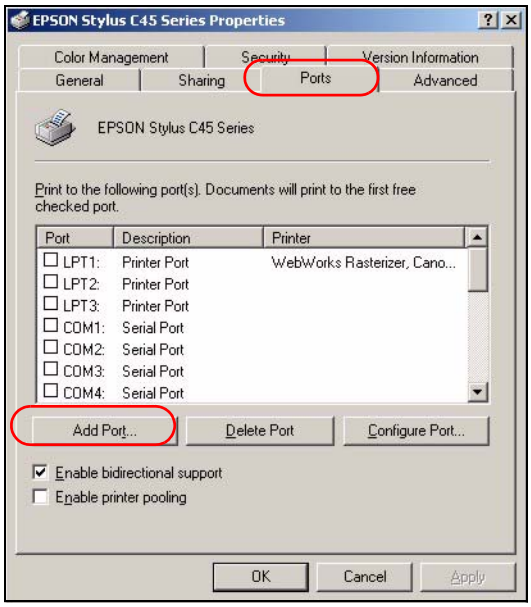
The **Printers** folder opens up. First you need to open up the properties windows for the printer you want to configure a TCP/IP port.

2 Locate your printer.

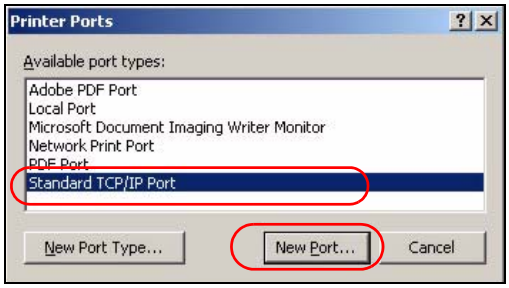
3 Right click on your printer and select **Properties**.



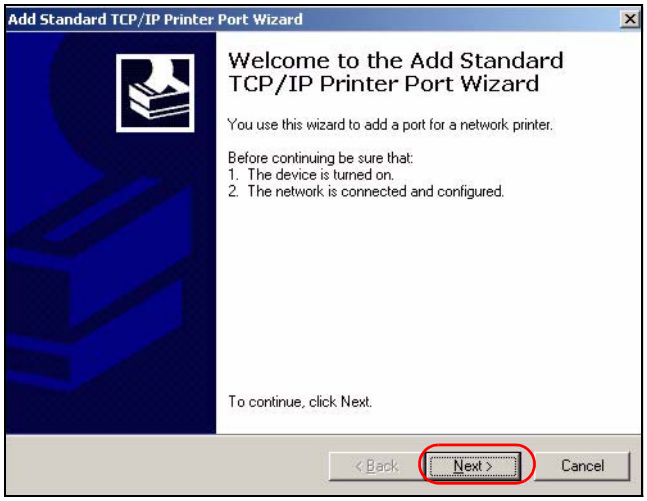
4 Select the **Ports** tab and click **Add Port...**



5 A **Printer Ports** window appears. Select **Standard TCP/IP Port** and click **New Port...**.

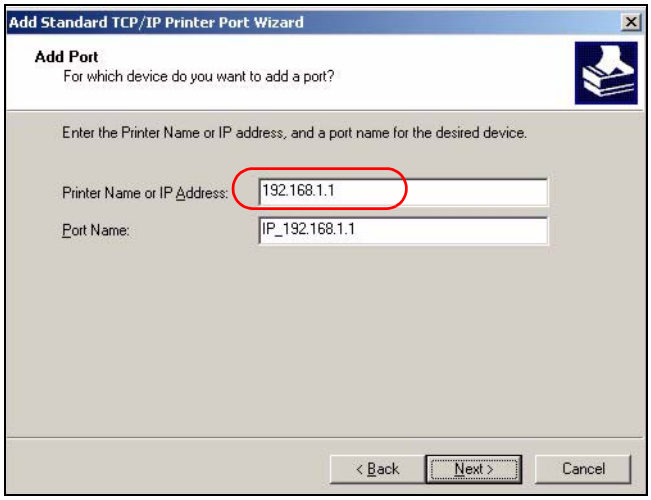


6 **Add Standard TCP/IP Printer Port Wizard** window opens up. Click **Next** to start configuring the printer port.

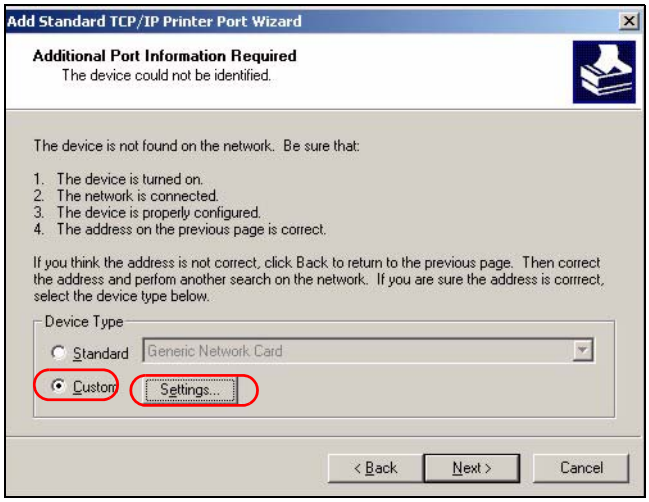

Add Standard TCP/IP Printer Port Wizard
Welcome to the Add Standard TCP/IP Printer Port Wizard
You use this wizard to add a port for a network printer.
Before continuing be sure that:
1. The device is turned on.
2. The network is connected and configured.
To continue, click Next.
< Back
Next >
Cancel

7 Enter the IP address of the ZyXEL Device to which the printer is connected in the **Printer Name or IP Address:** field. In our example we use the default IP address of the ZyXEL Device, 192.168.1.1. The **Port Name** field updates automatically to reflect the IP address of the port. Click **Next**.

Note: The computer from which you are configuring the TCP/IP printer port must be on the same LAN in order to use the printer sharing function.


Add Standard TCP/IP Printer Port Wizard
Add Port
For which device do you want to add a port?
Enter the Printer Name or IP address, and a port name for the desired device.
Printer Name or IP Address:
192.168.1.1
Port Name:
IP_192.168.1.1
< Back
Next >
Cancel

8 Select **Custom** under **Device Type** and click **Settings**.

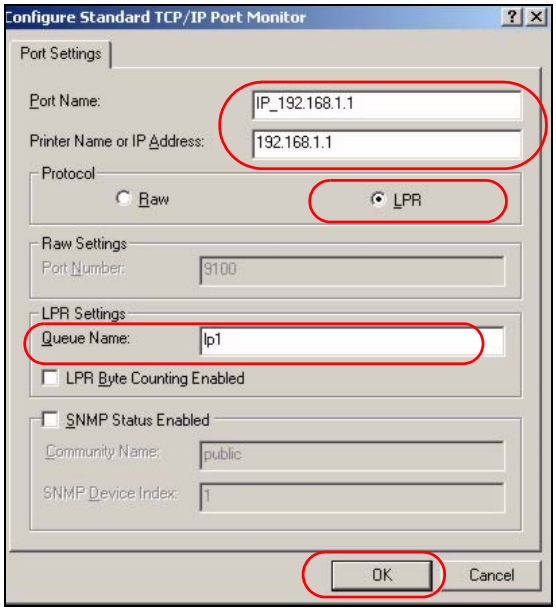

Add Standard TCP/IP Printer Port Wizard
Additional Port Information Required
The device could not be identified.
The device is not found on the network. Be sure that:
1. The device is turned on.
2. The network is connected.
3. The device is properly configured.
4. The address on the previous page is correct.
If you think the address is not correct, click Back to return to the previous page. Then correct the address and perfom another search on the network. If you are sure the address is correct, select the device type below.
Device Type
Standard
Generic Network Card
Custom
Settings...
< Back
Next >
Cancel

9 Confirm the IP address of the ZyXEL Device in the IP Address field.

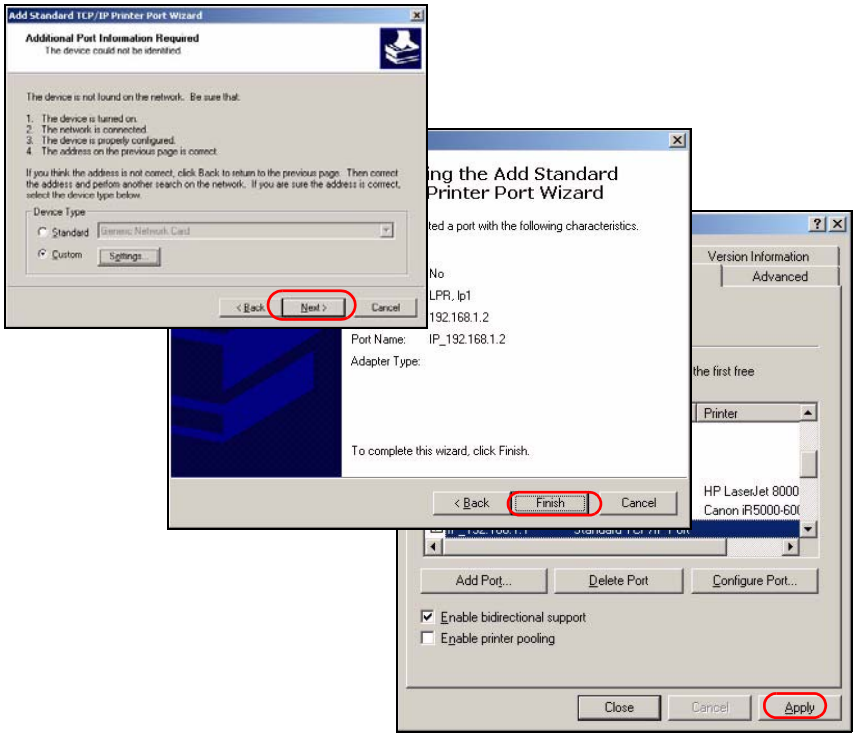
10 Select **LPR** under **Protocol**.

11 Type the LPR queue name of your printer model in the **Queue Name** field and click **OK**. Refer to your printer documentation for the LPR queue name. Some

printer models accept any name you want to use, in this case you can enter a short descriptive name for the **Queue Name**.



12 Continue through the wizard, apply your settings and close the wizard window.

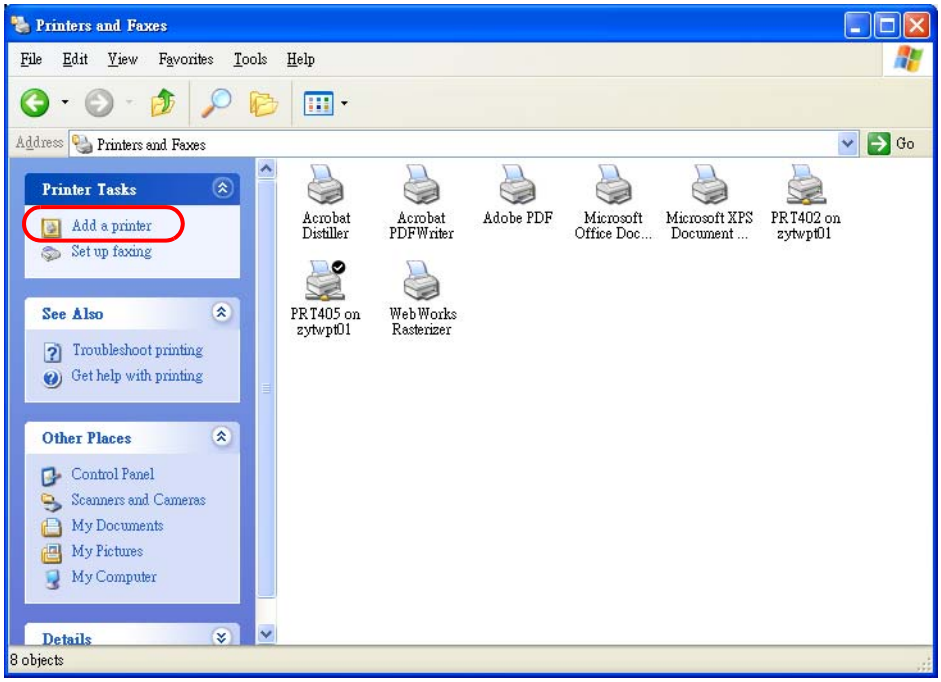


13 Repeat steps 1 to 12 to add this printer to other computers on your network.

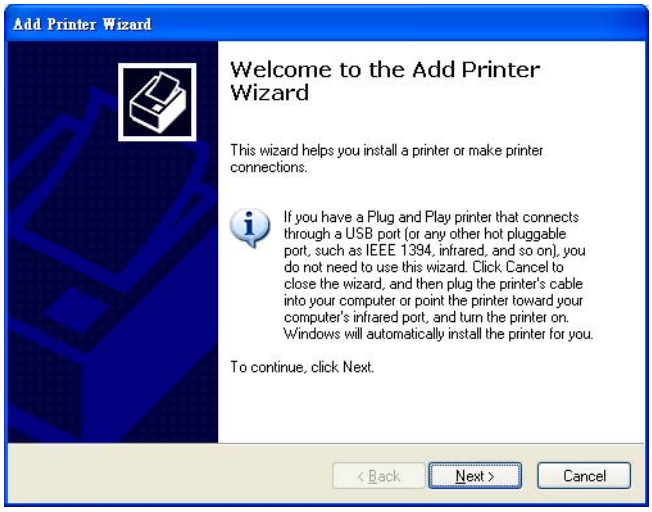
Add a New Printer Using Windows

This example shows how to connect a printer to your ZyXEL Device using the Windows XP Professional operating system. Some menu items may look different on your operating system.

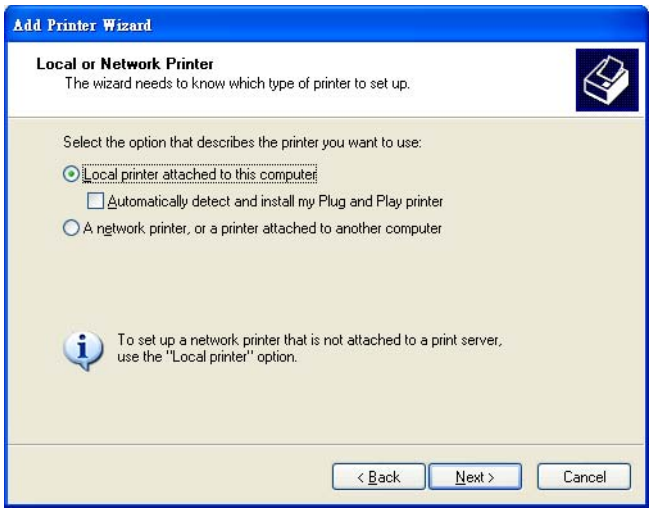
1 Click **Start** > **Control Panel** > **Printers and Faxes** to open the **Printers and Faxes** screen. Click **Add a Printer**.



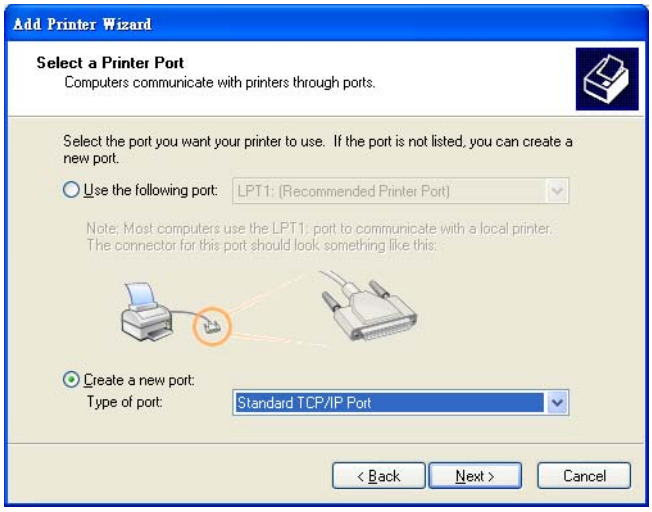
2 The **Add Printer Wizard** screen displays. Click **Next**.


Add Printer Wizard
Welcome to the Add Printer Wizard
This wizard helps you install a printer or make printer connections.
If you have a Plug and Play printer that connects through a USB port (or any other hot pluggable port, such as IEEE 1394, infrared, and so on), you do not need to use this wizard. Click Cancel to close the wizard, and then plug the printer's cable into your computer or point the printer toward your computer's infrared port, and turn the printer on. Windows will automatically install the printer for you.
To continue, click Next.
< Back
Next >
Cancel

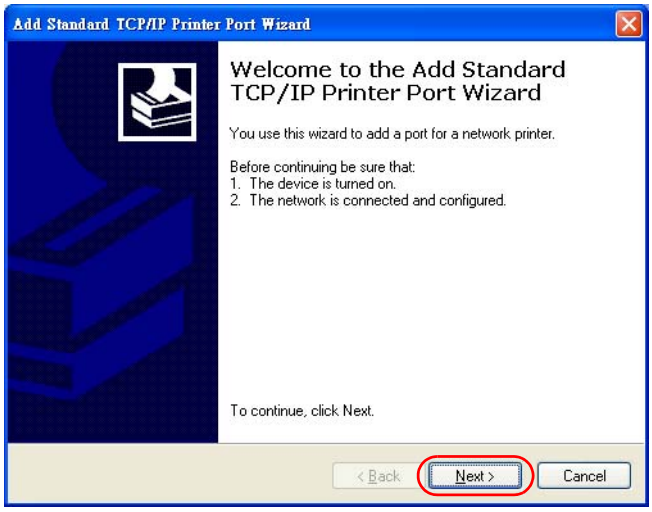
3 Select **Local printer attached to this computer** and click **Next**.


Add Printer Wizard
Local or Network Printer
The wizard needs to know which type of printer to set up.
Select the option that describes the printer you want to use:
Local printer attached to this computer
Automatically detect and install my Plug and Play printer
A network printer, or a printer attached to another computer
To set up a network printer that is not attached to a print server, use the "Local printer" option.
< Back
Next >
Cancel

4 Select **Create a new port** and **Standard TCP/IP Port**. Click **Next**.

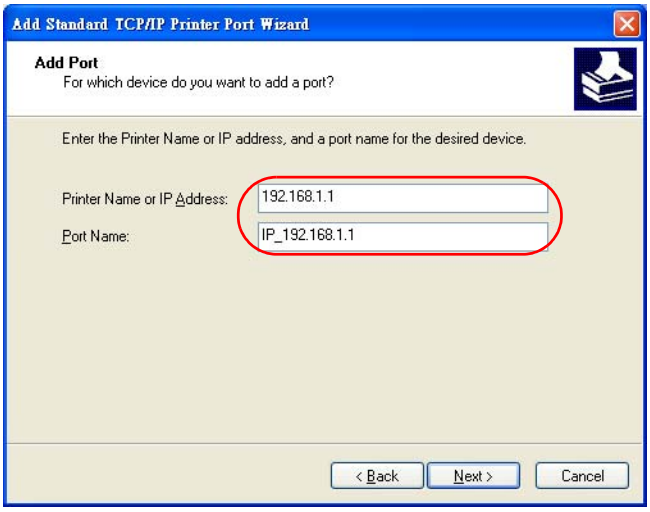

Add Printer Wizard
Select a Printer Port
Computers communicate with printers through ports.
Select the port you want your printer to use. If the port is not listed, you can create a new port.
Use the following port:
LPT1: (Recommended Printer Port)
Note: Most computers use the LPT1: port to communicate with a local printer. The connector for this port should look something like this:
Create a new port:
Type of port:
Standard TCP/IP Port
< Back
Next >
Cancel

5 **Add Standard TCP/IP Printer Port Wizard** window opens up. Click **Next** to start configuring the printer port.

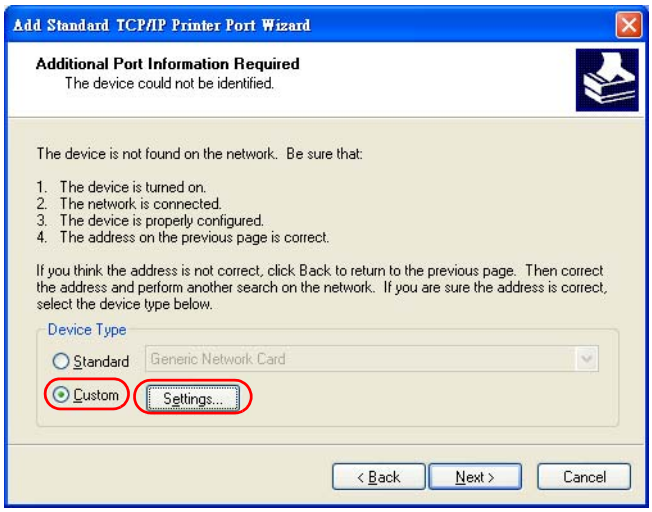

Add Standard TCP/IP Printer Port Wizard
Welcome to the Add Standard TCP/IP Printer Port Wizard
You use this wizard to add a port for a network printer.
Before continuing be sure that:
1. The device is turned on.
2. The network is connected and configured.
To continue, click Next.
< Back
Next >
Cancel

6 Enter the IP address of the ZyXEL Device to which the printer is connected in the **Printer Name or IP Address:** field. In our example we use the default IP address of the ZyXEL Device, 192.168.1.1. The **Port Name** field updates automatically to reflect the IP address of the port. Click **Next**.

Note: The computer from which you are configuring the TCP/IP printer port must be on the same LAN in order to use the printer sharing function.


Add Standard TCP/IP Printer Port Wizard
Add Port
For which device do you want to add a port?
Enter the Printer Name or IP address, and a port name for the desired device.
Printer Name or IP Address:
192.168.1.1
Port Name:
IP_192.168.1.1
< Back
Next >
Cancel

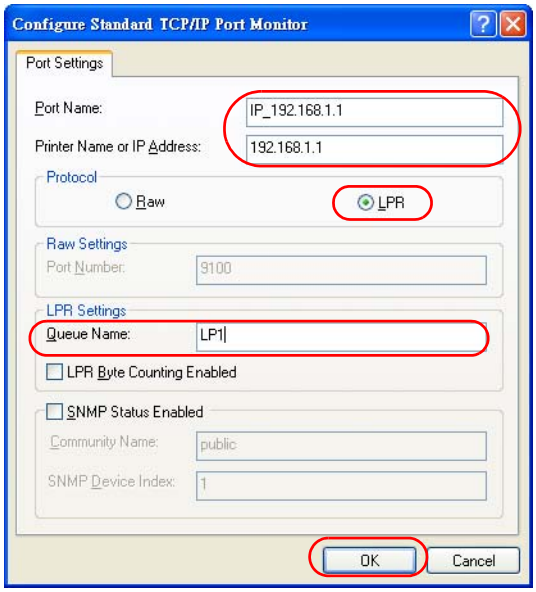
7 Select **Custom** under **Device Type** and click **Settings**.


Add Standard TCP/IP Printer Port Wizard
Additional Port Information Required
The device could not be identified.
The device is not found on the network. Be sure that:
1. The device is turned on.
2. The network is connected.
3. The device is properly configured.
4. The address on the previous page is correct.
If you think the address is not correct, click Back to return to the previous page. Then correct the address and perform another search on the network. If you are sure the address is correct, select the device type below.
Device Type
Standard
Generic Network Card
Custom
Settings...
< Back
Next >
Cancel

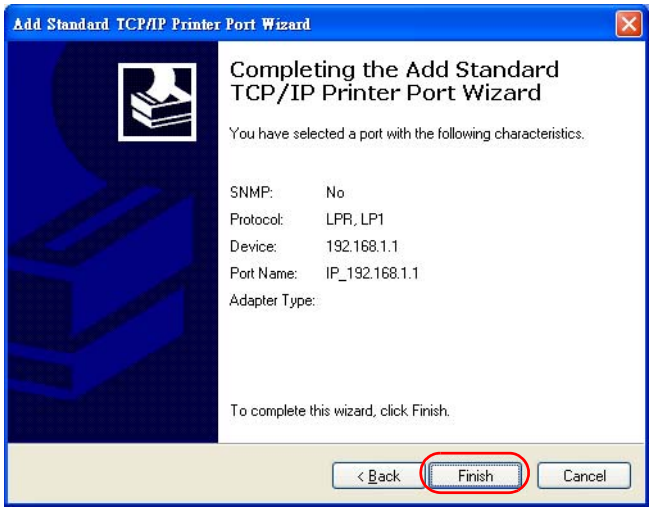
8 Confirm the IP address of the ZyXEL Device in the Printer **Name or IP Address** field.

9 Select **LPR** under **Protocol**.

10 Type **LP1** in the **Queue Name** field and click **OK** to go back to the previous screen and click **Next**.



11 Click **Finish** to close the wizard window.

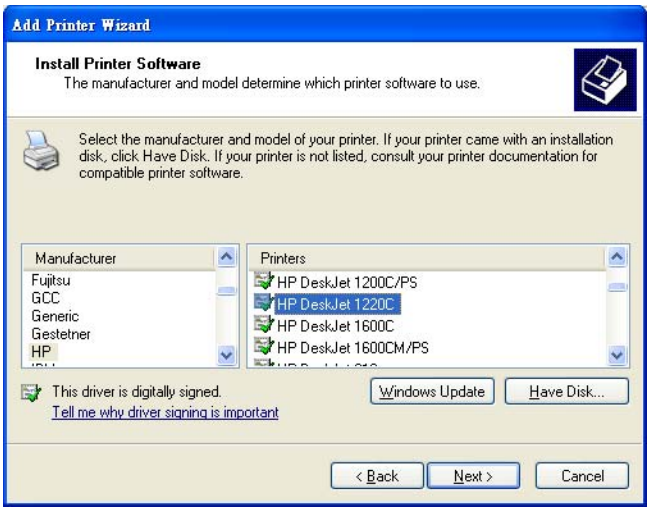


12 Select the make of the printer that you want to connect to the print server in the **Manufacturer** list of printers.

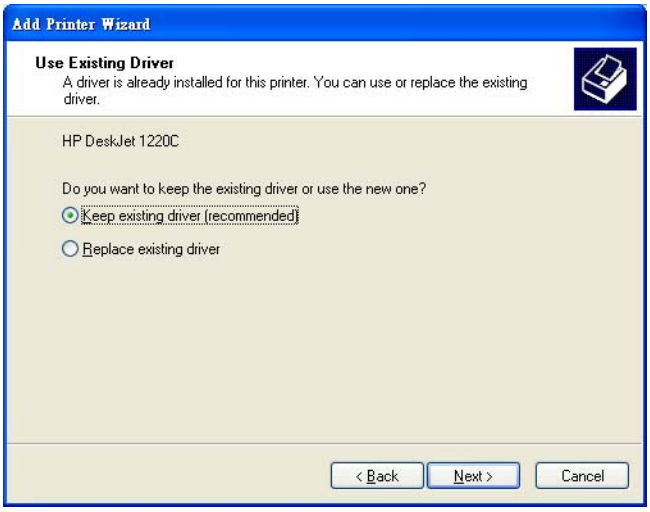
13 Select the printer model from the list of **Printers**.

14 If your printer is not displayed in the list of **Printers**, you can insert the printer driver installation CD/disk or download the driver file to your computer, click **Have Disk...** and install the new printer driver.

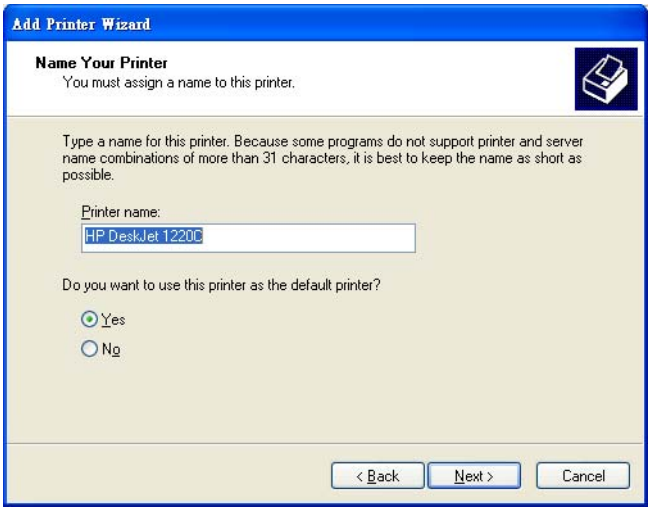
15 Click **Next** to continue.


Add Printer Wizard
Install Printer Software
The manufacturer and model determine which printer software to use.
Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for compatible printer software.
Manufacturer
Fujitsu
GCC
Generic
Gestetner
HP
Printers
HP DeskJet 1200C/PS
HP DeskJet 1220C
HP DeskJet 1600C
HP DeskJet 1600CM/PS
This driver is digitally signed.
Tell me why driver signing is important
Windows Update
Have Disk...
< Back
Next >
Cancel

16 If the following screen displays, select **Keep existing driver** radio button and click **Next** if you already have a printer driver installed on your computer and you do not want to change it. Otherwise, select **Replace existing driver** to replace it with the new driver you selected in the previous screen and click **Next**.

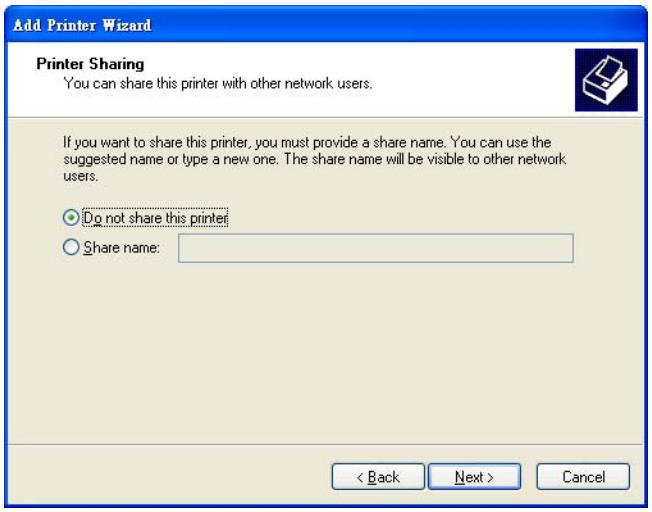

Add Printer Wizard
Use Existing Driver
A driver is already installed for this printer. You can use or replace the existing driver.
HP DeskJet 1220C
Do you want to keep the existing driver or use the new one?
Keep existing driver (recommended)
Replace existing driver
< Back
Next >
Cancel

17 Type a name to identify the printer and then click **Next** to continue.

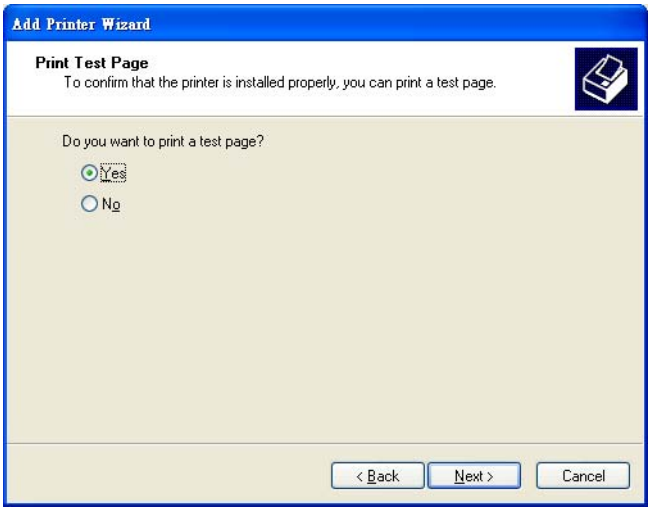

Add Printer Wizard
Name Your Printer
You must assign a name to this printer.
Type a name for this printer. Because some programs do not support printer and server name combinations of more than 31 characters, it is best to keep the name as short as possible.
Printer name:
HP DeskJet 1220C
Do you want to use this printer as the default printer?
Yes
No
< Back
Next >
Cancel

18 The ZyXEL Device is a print server itself and you do not need to have your computer act as a print server by sharing the printer with other users in the same

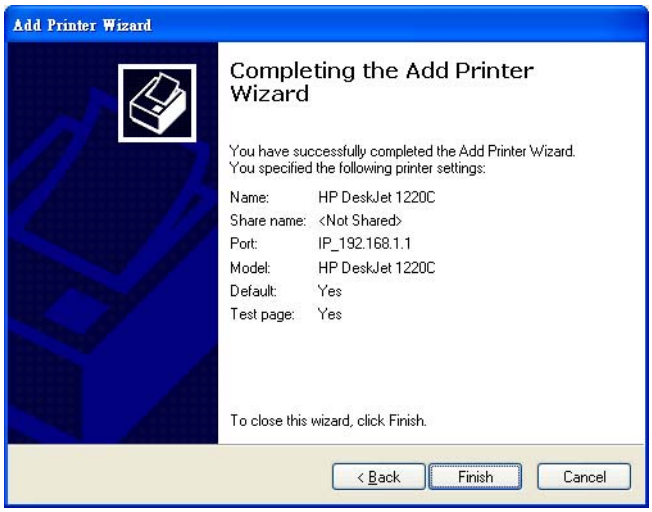
network; just select **Do not share this printer** and click **Next** to proceed to the following screen.


Add Printer Wizard
Printer Sharing
You can share this printer with other network users.
If you want to share this printer, you must provide a share name. You can use the suggested name or type a new one. The share name will be visible to other network users.
Do not share this printer
Share name:
< Back
Next >
Cancel

19 Select **Yes** and then click the **Next** button if you want to print a test page. A pop-up screen displays to ask if the test page printed correctly. Otherwise select **No** and then click **Next** to continue.


Add Printer Wizard
Print Test Page
To confirm that the printer is installed properly, you can print a test page.
Do you want to print a test page?
Yes
No
< Back
Next >
Cancel

20 The following screen shows your current printer settings. Select **Finish** to complete adding a new printer.



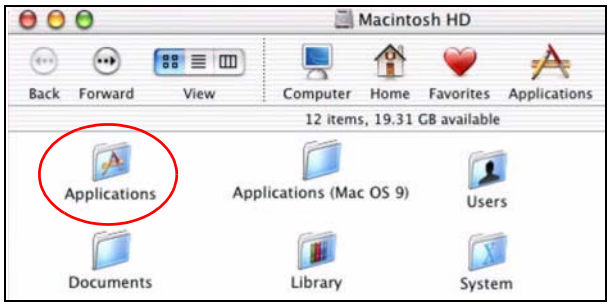
Add a New Printer Using Macintosh OS X

Complete the following steps to set up a print server driver on your Macintosh computer.

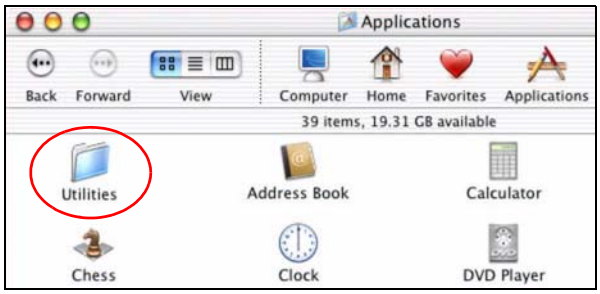
1 Click the **Print Center** icon located in the Macintosh Dock (a place holding a series of icons/shortcuts at the bottom of the desktop). Proceed to step 6 to continue. If the **Print Center** icon is not in the Macintosh Dock, proceed to the next step.

2 On your desktop, double-click the **Macintosh HD** icon to open the **Macintosh HD** window.

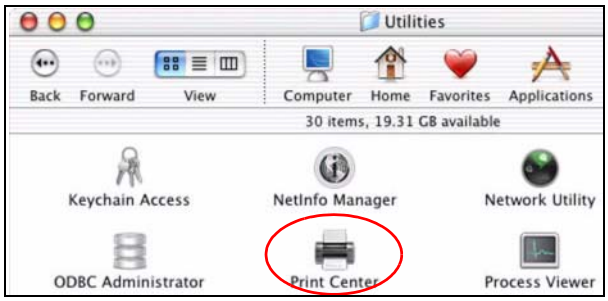
3 Double-click the **Applications** folder.



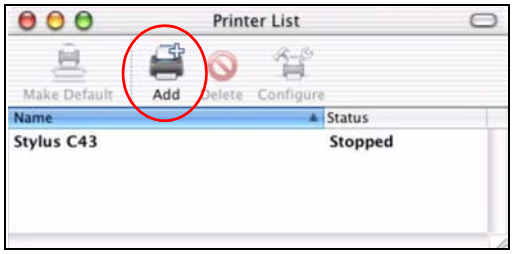
4 Double-click the **Utilities** folder.



5 Double-click the **Print Center** icon.



6 Click the **Add** icon at the top of the screen.



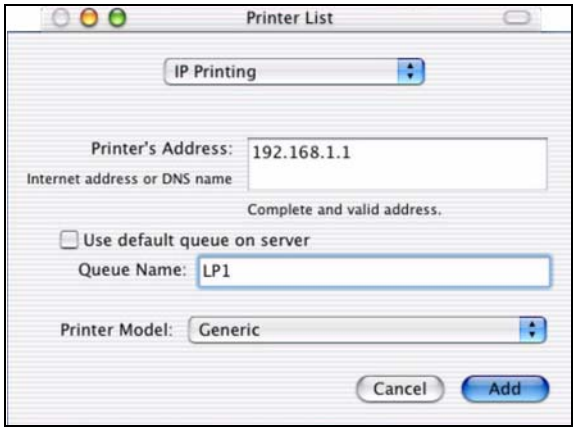
7 Set up your printer in the **Printer List** configuration screen. Select **IP Printing** from the drop-down list box.

8 In the **Printer's Address** field, type the IP address of your ZyXEL Device.

9 Deselect the **Use default queue on server** check box.

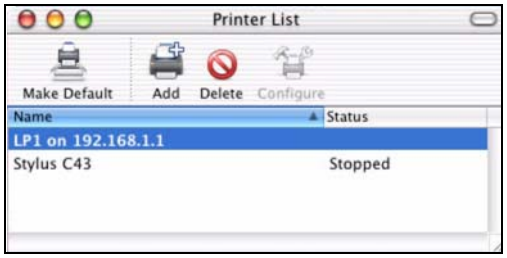
10 Type **LP1** (a parallel port) in the **Queue Name** field.

11 Select your **Printer Model** from the drop-down list box. If the printer's model is not listed, select **Generic**.



12 Click **Add** to select a printer model, save and close the **Printer List** configuration screen.

13 The **Name LP1 on 192.168.1.1** displays in the **Printer List** field. The default printer **Name** displays in bold type.

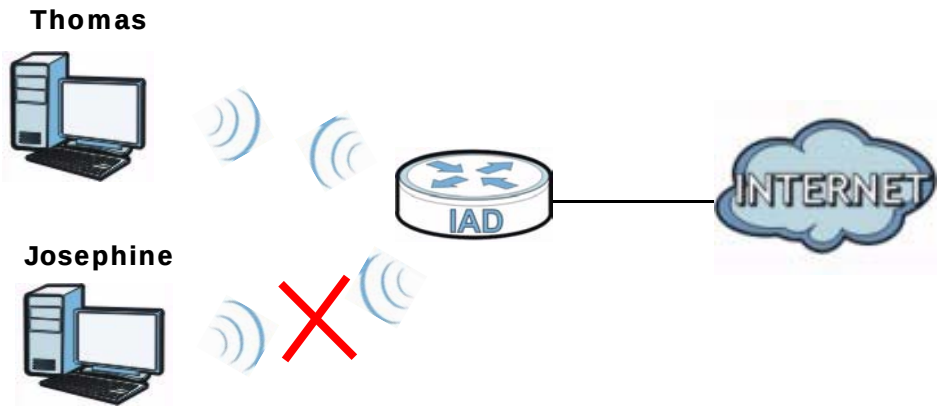


Your Macintosh print server driver setup is complete. You can now use the ZyXEL Device's print server to print from a Macintosh computer.

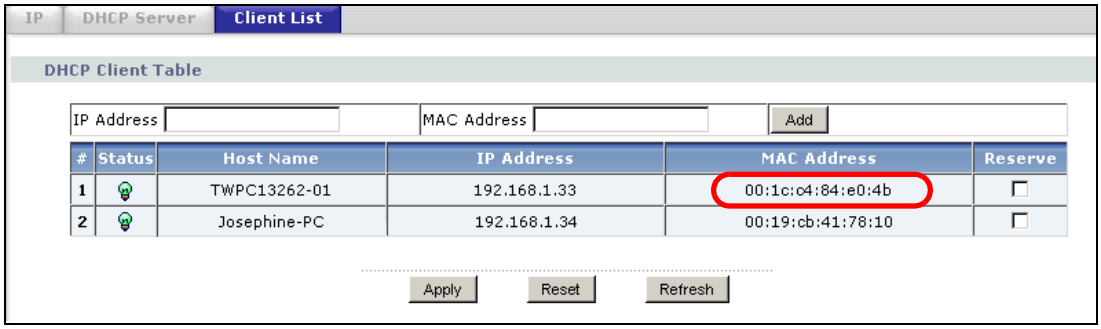
3.9 Configuring the MAC Address Filter

Thomas noticed that his daughter Josephine spends too much time surfing the web and downloading media files. He decided to prevent Josephine from accessing the Internet so that she can concentrate on preparing for her final exams.

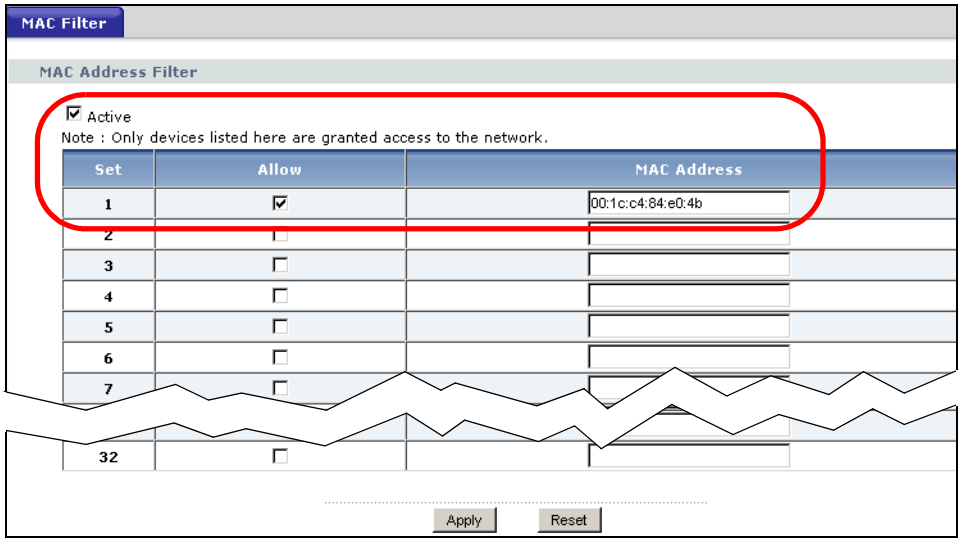
Josephine's computer connects wirelessly to the Internet through the ZyXEL Device. Thomas decides to use the **Security > MAC Filter** screen to grant wireless network access to his computer but not to Josephine's computer.



1 Click **Network** > **LAN** > **Client List** to open the following screen. Look for the MAC address of Thomas' computer.



2 Click **Security** > **MAC Filter** to open the **MAC Filter** screen. Select **Active**. Enter the MAC address you found in the **Client List** screen. Click **Apply**.



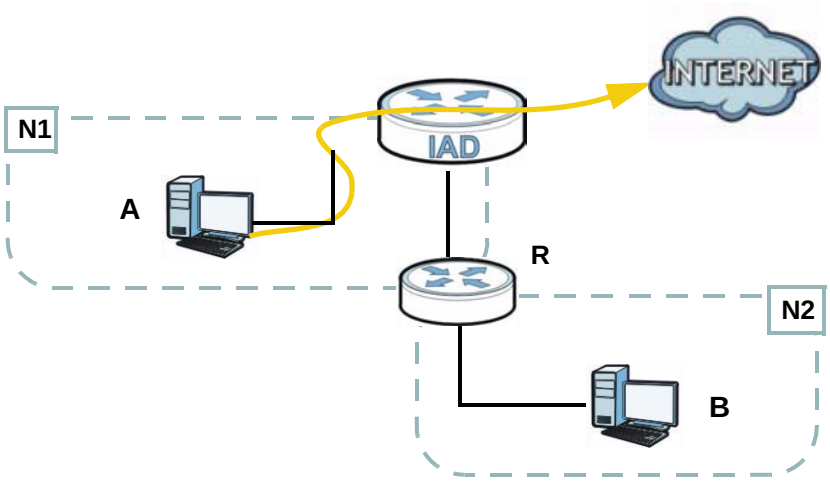
Thomas can also grant access to the computers of other members of his family and friends. However, Josephine and others not listed in this screen will no longer be able to access the Internet through the ZyXEL Device.

3.10 Configuring Static Route for Routing to Another Network

In order to extend your Intranet and control traffic flowing directions, you may connect a router to the ZyXEL Device's LAN. The router may be used to separate two department networks. This tutorial shows how to configure a static routing rule for two network routings.

In the following figure, router **R** is connected to the ZyXEL Device's LAN. **R** connects to two networks, **N1** (192.168.1.x/24) and **N2** (192.168.10.x/24). If you want to send traffic from computer **A** (in **N1** network) to computer **B** (in **N2**

network), the traffic is sent to the ZyXEL Device's WAN default gateway by default. In this case, **B** will never receive the traffic.



You need to specify a static routing rule on the ZyXEL Device to specify **R** as the router in charge of forwarding traffic to **N2**. In this case, the ZyXEL Device routes traffic from **A** to **R** and then **R** routes the traffic to **B**.This tutorial uses the following example IP settings:

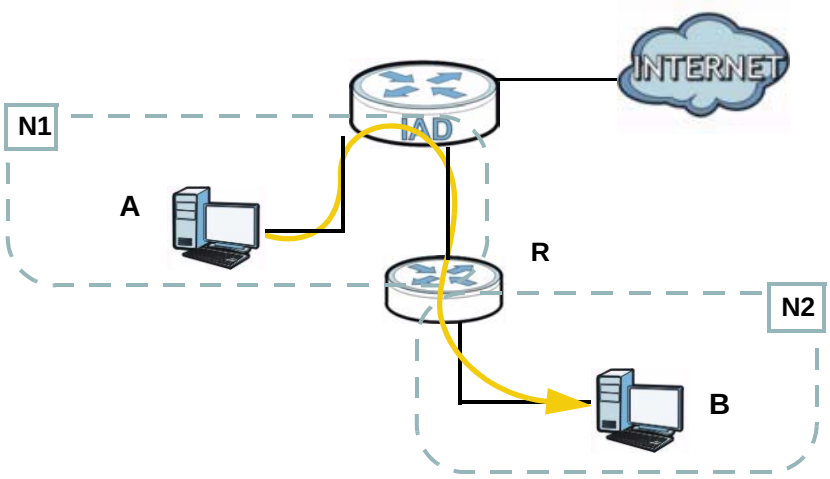


Table 3 IP Settings in this Tutorial

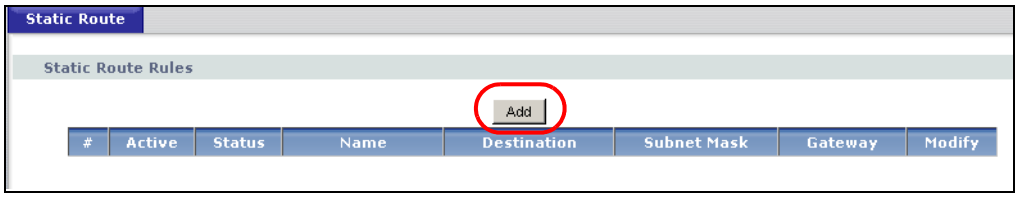
DEVICE / COMPUTER	IP ADDRESS
The ZyXEL Device's WAN	172.16.1.1
The ZyXEL Device's LAN	192.168.1.1
A	192.168.1.34
R's N1	192.168.1.253

Table 3 IP Settings in this Tutorial

DEVICE / COMPUTER	IP ADDRESS
R's N2	192.168.10.2
B	192.168.10.33

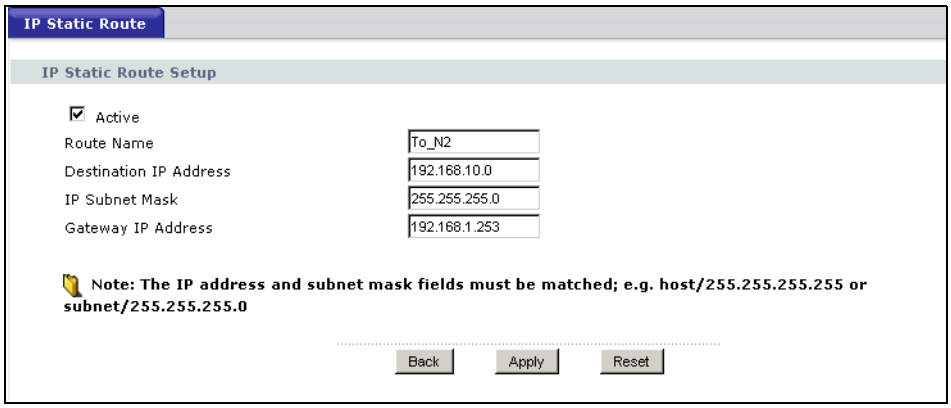
To configure a static route to route traffic from **N1** to **N2**:

1 Click **Advanced** > **Static Route**. Click **Add**.

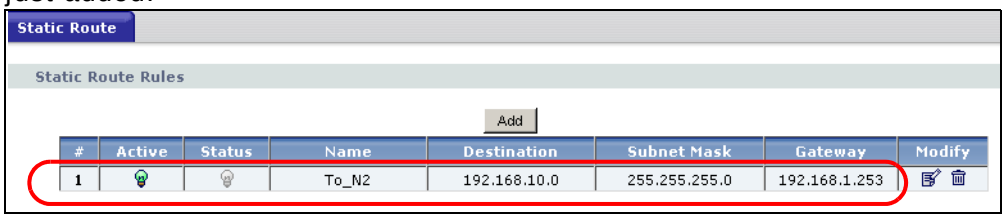


2 Configure the **Static Route Setup** screen using the following settings:

- Select **Active**.
- Specify a descriptive name for this routing rule.
- Type **192.168.10.0** and subnet mask **255.255.255.0** for the destination, **N2**.
- Type **192.168.1.253** (**R**'s N1 address) in the **Gateway IP Address** field.



Click **Apply**. The **Advanced** > **Static Route** screen should display the route you just added.


Static Route
Static Route Rules
Add
Active Status Name Destination Subnet Mask Gateway Modify
1 To_N2 192.168.10.0 255.255.255.0 192.168.1.253

Now **B** should be able to receive traffic from **A**. You may need to additionally configure **B**'s firewall settings to allow specific traffic to pass through.

3.11 Configuring QoS Queue and Class Setup

This section contains tutorials on how you can configure the QoS screen.

Note: Voice traffic will not be affected by the user-defined QoS settings on the ZyXEL Device. It always gets the highest priority.

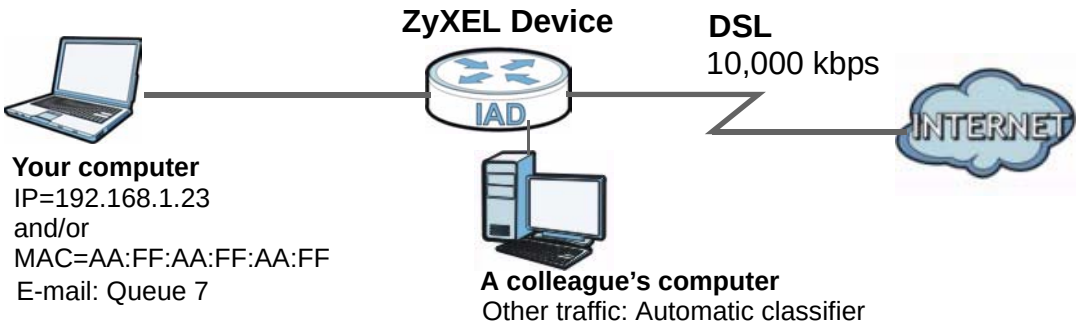
Let's say you are a team leader of a small sales branch office. You want to prioritize e-mail traffic because your task includes sending urgent updates to clients at least twice every hour. You also upload data files (such as logs and e-mail archives) to the FTP server throughout the day. Your colleagues use the Internet for research, as well as chat applications for communicating with other branch offices.

In the following figure, your Internet connection has an upstream transmission bandwidth of 10,000 kbps. For this example, you want to configure QoS so that e-mail traffic gets the highest priority with at least 5,000 kbps. You can do the following:

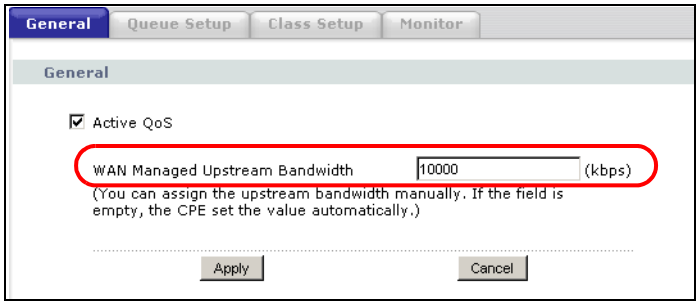
- Configure a queue to assign the highest priority queue (7) to e-mail traffic from the LAN interface, so that e-mail traffic would not get delayed when there is network congestion.
- Note the IP address (192.168.1.23 for example) and/or MAC address (AA:FF:AA:FF:AA:FF for example) of your computer and map it to queue 7.

Note: QoS is applied to traffic flowing out of the ZyXEL Device.

Traffic that does not match this class is assigned a priority queue based on the internal QoS mapping table on the ZyXEL Device.

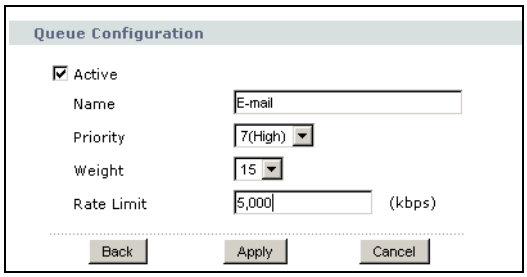


1 Click **Advanced > QoS > General** and check **Active**. Set your **WAN Managed Upstream Bandwidth** to 10,000 kbps (or leave this blank to have the ZyXEL Device automatically determine this figure).

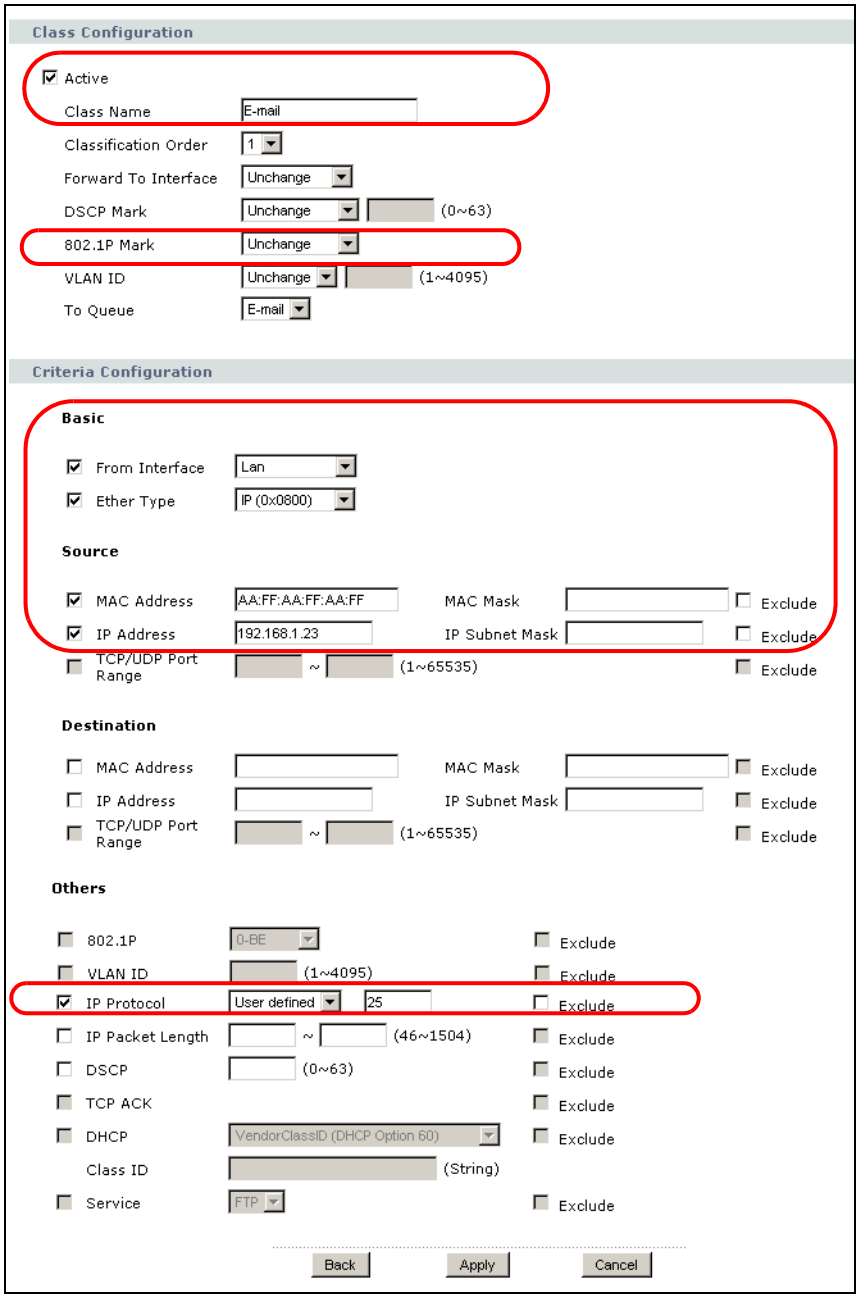


2 Go to **Advanced > QoS > Queue Setup**. Click **Add** to create a new queue. In the screen that opens, check **Active** and enter or select the following values:

- **Name**: E-mail
- **Priority**: 7 (High)
- **Weight**: 15
- **Rate Limit**: 5,000 (kbps)



3 Go to **Advanced > QoS > Class Setup**. Click **Add** to create a new class. Check **Active** and follow the settings as shown in the screen below.

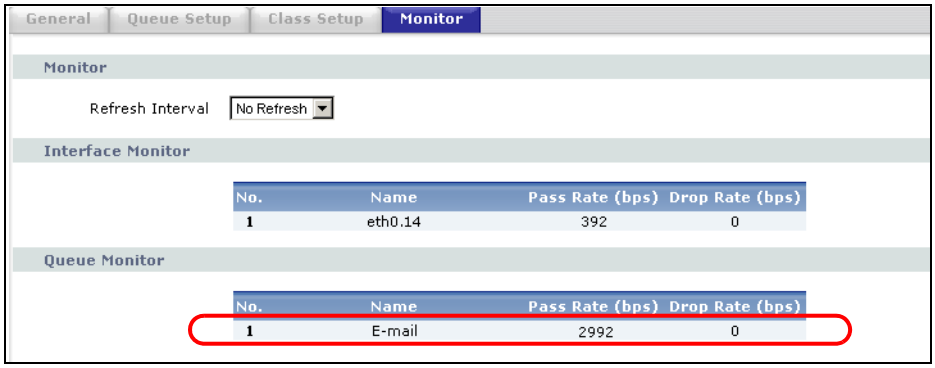


Class Name	Give a class name to this traffic, such as **E-mail** in this example.
To Queue	Link this to an item in the **QoS > Queue Setup** screen, which is the **E-mail** queue created in this example.
From Interface	This is the interface from which the traffic will be coming from. Select **LAN**.

Ether Type	Select **IP** to identify the traffic source by its IP address or MAC address.
MAC Address	Type the MAC address of your computer - **AA:FF:AA:FF:AA:FF**. Type the **MAC Mask** if you know it.
IP Address	Type the IP address of your computer - **192.168.1.23**. Type the **IP Subnet Mask** if you know it.

This maps e-mail traffic to queue 7 created in the previous screen (see the **IP Protocol** field). This also maps your computer's IP address and MAC address to queue 7 (see the **Source** fields).

4 Verify that the queue setup works by checking **Advanced > QoS > Monitor**. This shows the bandwidth allotted to e-mail traffic compared to other network traffic.



3.12 Access the ZyXEL Device Using DDNS

If you connect your ZyXEL Device to the Internet and it uses a dynamic WAN IP address, it is inconvenient for you to manage the device from the Internet. The ZyXEL Device's WAN IP address changes dynamically. Dynamic DNS (DDNS) allows you to access the ZyXEL Device using a domain name.

To use this feature, you have to apply for DDNS service at www.dyndns.org.

This tutorial shows you how to:

- Registering a DDNS Account on www.dyndns.org
- Configuring DDNS on Your ZyXEL Device
- Testing the DDNS Setting

Note: If you have a private WAN IP address, then you cannot use DDNS.

3.12.1 Registering a DDNS Account on www.dyndns.org

1. Open a browser and type **http://www.dyndns.org**.
2. Apply for a user account. This tutorial uses **UserName1** and **12345** as the username and password.
3. Log into www.dyndns.org using your account.
4. Add a new DDNS host name. This tutorial uses the following settings as an example.
   - Hostname: **zyxelrouter.dyndns.org**
   - Service Type: **Host with IP address**
   - IP Address: Enter the WAN IP address that your ZyXEL Device is currently using. You can find the IP address on the ZyXEL Device's Web Configurator **Status** page.

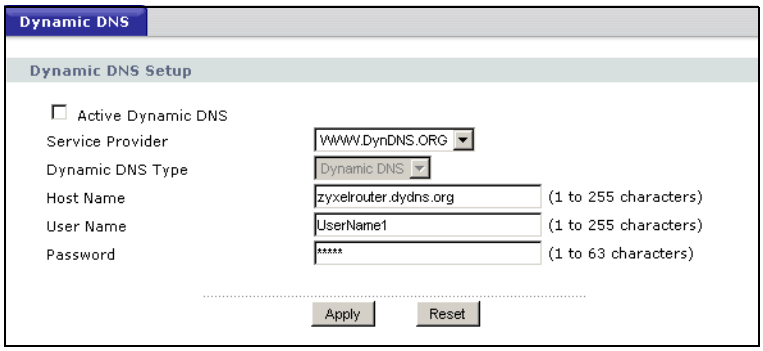
   Then you will need to configure the same account and host name on the ZyXEL Device later.

3.12.2 Configuring DDNS on Your ZyXEL Device

Configure the following settings in the **Advanced** > **Dynamic DNS** screen.

- Select **Active Dynamic DNS**.
- Select **Dynamic DNS** for the DDNS type.
- Type **zyxelrouter.dyndns.org** in the **Host Name** field.

- Enter the user name (**UserName1**) and password (**12345**).



Click **Apply**.

3.12.3 Testing the DDNS Setting

Now you should be able to access the ZyXEL Device from the Internet. To test this:

1. Open a web browser on the computer (using the IP address **a.b.c.d**) that is connected to the Internet.
2. Type **http://zyxelrouter.dyndns.org** and press [Enter].
3. The ZyXEL Device's login page should appear. You can then log into the ZyXEL Device and manage it.

PART II
Advanced

Status Screens (85)

WAN Setup (97)

LAN Setup (121)

Wireless LAN (129)

Network Address Translation (NAT) (149)

Voice (157)

File Sharing (183)

Media Server (193)

Print Server (195)

MAC Filter (201)

Firewall (203)

Certificates (209)

Static Route (219)

Quality of Service (QoS) (223)

Dynamic DNS Setup (237)

Service Control (239)

4

Status Screens

4.1 Status Overview

Use the **Status** screens to look at the current status of the device, system resources, interfaces (LAN, WAN and WLAN), and SIP accounts. You can also register and unregister SIP accounts. The **Status** screen also provides detailed information from DHCP and statistics from VoIP, and traffic.

Click **Status** to open this screen. The screen varies slightly depending on the WAN mode you set using the **DSL / WAN** switch.

Figure 7 Status Screen (ADSL WAN mode)

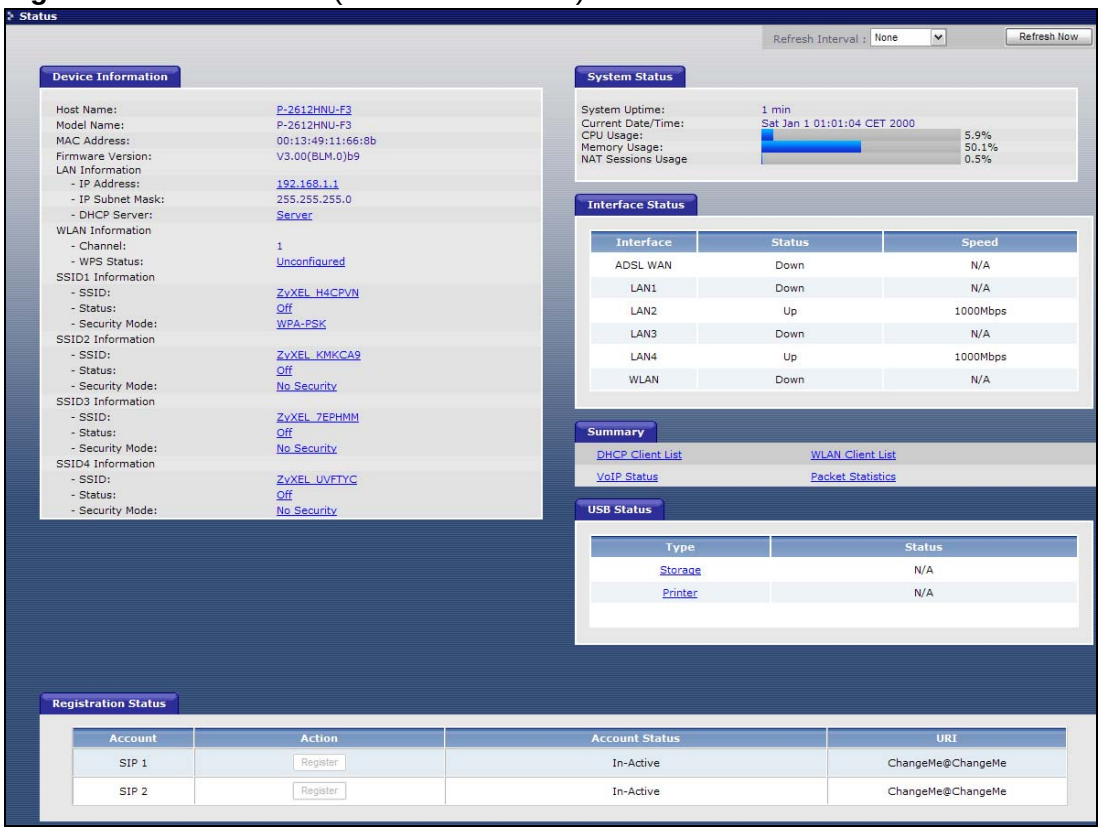
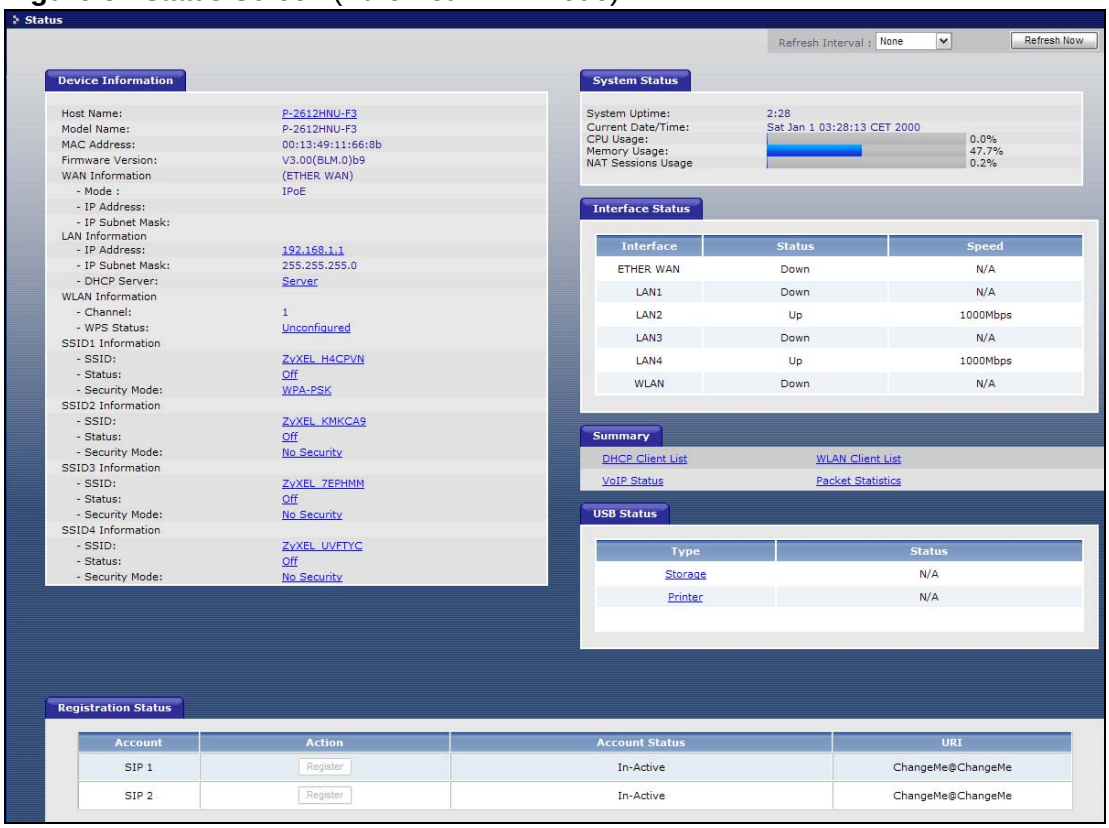


Figure 8 Status Screen (Ethernet WAN mode)



Each field is described in the following table.

Table 4 Status Screen

LABEL	DESCRIPTION
Refresh Interval	Enter how often you want the ZyXEL Device to update this screen.
Refresh Now	Click this to update this screen immediately.
Device Information	
Host Name	This field displays the ZyXEL Device system name. It is used for identification. You can change this in the **Maintenance > System > General** screen's **System Name** field.
Model Name	This is the model name of your device.
MAC Address	This is the MAC (Media Access Control) or Ethernet address unique to your ZyXEL Device.
Firmware Version	This field displays the current version of the firmware inside the device. It also shows the date the firmware version was created. Click this to go to the screen where you can change it.
WAN Information	
Mode	This field is not available when the WAN mode is **Ethernet WAN**. This is the DSL standard that your ZyXEL Device is using.

LABEL	DESCRIPTION
IP Address	This field displays the current IP address of the ZyXEL Device in the WAN. Click this to go to the screen where you can change it.
IP Subnet Mask	This field displays the current subnet mask in the WAN.
LAN Information	
IP Address	This field displays the current IP address of the ZyXEL Device in the LAN. Click this to go to the screen where you can change it.
IP Subnet Mask	This field displays the current subnet mask in the LAN.
DHCP Server	This field displays what DHCP services the ZyXEL Device is providing to the LAN. Choices are: **Server** - The ZyXEL Device is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN. **Relay** - The ZyXEL Device acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. **None** - The ZyXEL Device is not providing any DHCP services to the LAN. Click this to go to the screen where you can change it.
WLAN Information	
Channel	This is the channel number used by the ZyXEL Device now.
Security	This displays the type of security mode the ZyXEL Device is using in the wireless LAN.
WPS Status	**Configured** displays when a wireless client has connected to the ZyXEL Device or WPS is enabled and wireless or wireless security settings have been configured. **Unconfigured** displays if WPS is disabled or wireless security settings have not been configured.
SSID (1~4) Information	
SSID	This is the descriptive name used to identify the ZyXEL Device in the wireless LAN. Click this to go to the screen where you can change it.
Status	This shows whether or not the SSID is enabled (on).
Security Mode	This displays the type of security the ZyXEL Device is using in the wireless LAN.
System Status	
System Uptime	This field displays how long the ZyXEL Device has been running since it last started up. The ZyXEL Device starts up when you plug it in, when you restart it (**Maintenance > Tools > Restart**), or when you reset it (see Section 1.6 on page 26).
Current Date/Time	This field displays the current date and time in the ZyXEL Device. You can change this in **Maintenance > System > Time Setting**.
System Mode	This displays whether the ZyXEL Device is functioning as a router or a bridge.

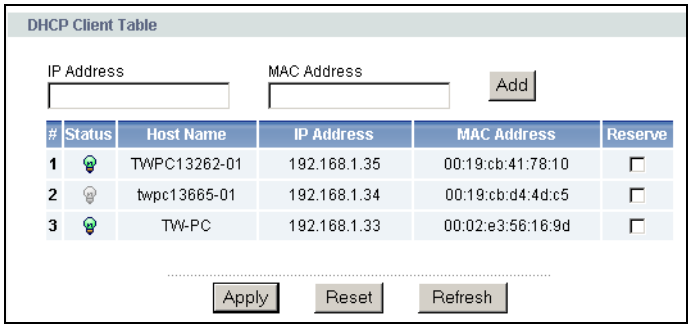
LABEL	DESCRIPTION
CPU Usage	This field displays what percentage of the ZyXEL Device's processing ability is currently used. When this percentage is close to 100%, the ZyXEL Device is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications.
Memory Usage	This field displays what percentage of the ZyXEL Device's memory is currently used. Usually, this percentage should not increase much. If memory usage does get close to 100%, the ZyXEL Device is probably becoming unstable, and you should restart the device. See Section 22.4 on page 259, or turn off the device (unplug the power) for a few seconds.
NAT Sessions Usage	This field displays what percentage of traffic passing through the ZyXEL Device is using NAT.
Interface Status	
Interface	This column displays each interface the ZyXEL Device has.
Status	This field indicates whether or not the ZyXEL Device is using the interface. For the DSL interface, this field displays **Down** (line is down), **Up** (line is up or connected) if you're using Ethernet encapsulation and **Down** (line is down), **Up** (line is up or connected), **Idle** (line (ppp) idle), **Dial** (starting to trigger a call) and **Drop** (dropping a call) if you're using PPPoE encapsulation. For the WAN interface, this field displays **Up** when the ZyXEL Device is using the interface and **Down** when the ZyXEL Device is not using the interface. For the LAN interface, this field displays **Up** when the ZyXEL Device is using the interface and **Down** when the ZyXEL Device is not using the interface. For the WLAN interface, it displays **Active** when WLAN is enabled or **InActive** when WLAN is disabled.
Speed	For the LAN interface, this displays the port speed and duplex setting. For the WAN interface, this displays the port speed and duplex setting. For the DSL interface, it displays the downstream and upstream transmission rate. For the WLAN interface, it displays the maximum transmission rate when WLAN is enabled or **N/A** when WLAN is disabled.
Summary	
DHCP Client List	Click this link to view current DHCP client information. See Section 6.4 on page 124.
WLAN Client List	Click this link to display the MAC address(es) of the wireless stations that are currently associating with the ZyXEL Device. See Section 4.2 on page 90.
VoIP Status	Click this link to view statistics about your VoIP usage. See Section 4.5 on page 93.
Packet Statistics	Click this link to view port status and packet specific statistics. See Section 4.4 on page 92.

LABEL	DESCRIPTION
USB Status	
Type	This shows the type of device connected to the ZyXEL Device.
Status	This shows whether the device is currently active (**Up**). This shows **N/A** if there are no device connected to the ZyXEL Device or the connected device is not working.
Registration Status	
Account	This column displays each SIP account in the ZyXEL Device.
Action	This field displays the current registration status of the SIP account. You have to register SIP accounts with a SIP server to use VoIP. If the SIP account is already registered with the SIP server, • Click **Unregister** to delete the SIP account's registration in the SIP server. This does not cancel your SIP account, but it deletes the mapping between your SIP identity and your IP address or domain name. • The second field displays **Registered**. If the SIP account is not registered with the SIP server, • Click **Register** to have the ZyXEL Device attempt to register the SIP account with the SIP server. • The second field displays the reason the account is not registered. **Inactive** - The SIP account is not active. You can activate it in **VoIP > SIP > SIP Settings**. **Register Fail** - The last time the ZyXEL Device tried to register the SIP account with the SIP server, the attempt failed. The ZyXEL Device automatically tries to register the SIP account when you turn on the ZyXEL Device or when you activate it.
Account Status	This shows **Active** when the SIP account has been registered and ready for use or **In-Active** when the SIP account is not yet registered.
URI	This field displays the account number and service domain of the SIP account. You can change these in **VoIP > SIP > SIP Settings**.

4.2 DHCP Client List

Use this table to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.

Figure 9 Network > LAN > Client List



The following table describes the labels in this screen.

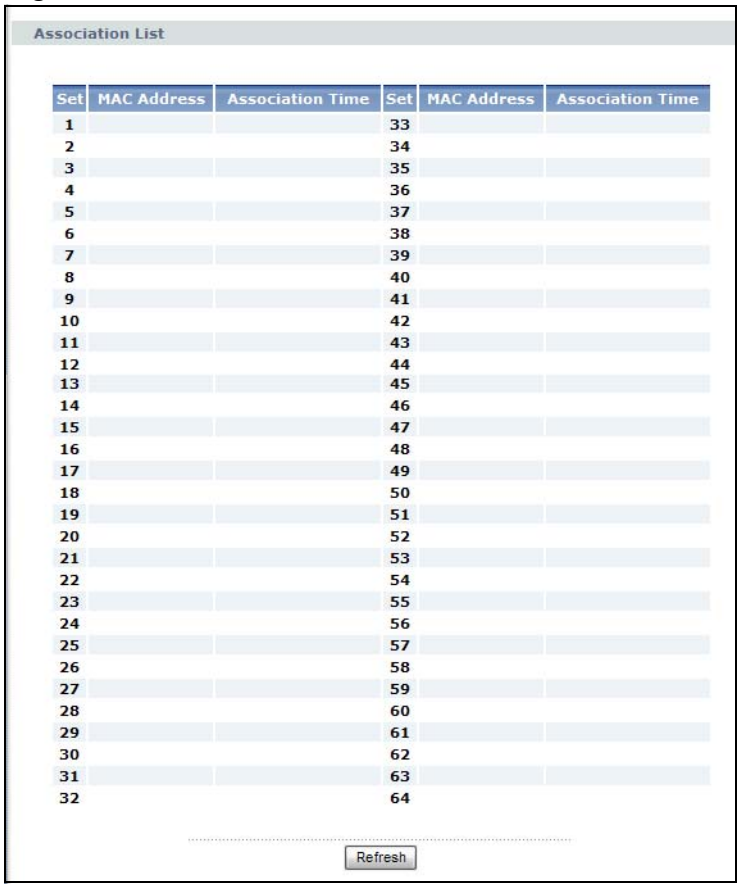
Table 5 Network > LAN > Client List

LABEL	DESCRIPTION
IP Address	Enter the IP address that you want to assign to the computer on your LAN with the MAC address that you will also specify.
MAC Address	Enter the MAC address of a computer on your LAN.
Add	Click **Add** to add a static DHCP entry.
#	This is the index number of the static IP table entry (row).
Status	This field displays whether the client is connected to the ZyXEL Device.
Host Name	This field displays the computer host name.
IP Address	This field displays the IP address relative to the # field listed above.
MAC Address	The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation). A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
Reserve	Select the check box in the heading row to automatically select all check boxes or select the check box(es) in each entry to have the ZyXEL Device always assign the selected entry(ies)'s IP address(es) to the corresponding MAC address(es) (and host name(s)). You can select up to 128 entries in this table.
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to begin configuring this screen afresh.
Refresh	Click this to reload the DHCP table.

4.3 WLAN Client List

Click **Status > WLAN Status** to access this screen. Use this screen to view the wireless stations that are currently associated to the ZyXEL Device.

Figure 10 WLAN Status



The following table describes the labels in this screen.

Table 6 WLAN Status

LABEL	DESCRIPTION
Set	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC (Media Access Control) address of an associated wireless station.
Association TIme	This field displays the time a wireless station first associated with the ZyXEL Device.
Refresh	Click this to reload this screen.

4.4 Packet Statistics

Click **Status > Packet Statistics** to access this screen. Read-only information here includes port status and packet specific statistics. Also provided are "system up time" and "poll interval(s)". The **Poll Interval(s)** field is configurable. The screen varies slightly depending on the WAN mode you set using the **DSL/WAN** switch.

Figure 11 Packet Statistics

The following table describes the fields in this screen.

Table 7 Packet Statistics

LABEL	DESCRIPTION
WAN Services Statistics	
Interface	This shows the name of the interface. For the WAN interface a default name **nas** followed by a number (for example, **nas1**) indicates the DSL interface. The name **eth0.14** indicates the default Ethernet WAN interface (the physical Ethernet WAN port). The number after the dot (**.**) represents the VLAN ID number assigned to traffic sent through this connection.
Description	This applies to the WAN connection and shows the service name of the WAN connection. 1 and 2 or 0 and 1 are the default VPI and VCI numbers. The last number represents the index number of connections over the same PVC or the VLAN ID number assigned to traffic sent through this connection.
Received Bytes	This field displays the number of bytes received on this port.
Pkts	This field displays the number of packets received on this port.
Errs	This field displays the number of error packets received on this port.

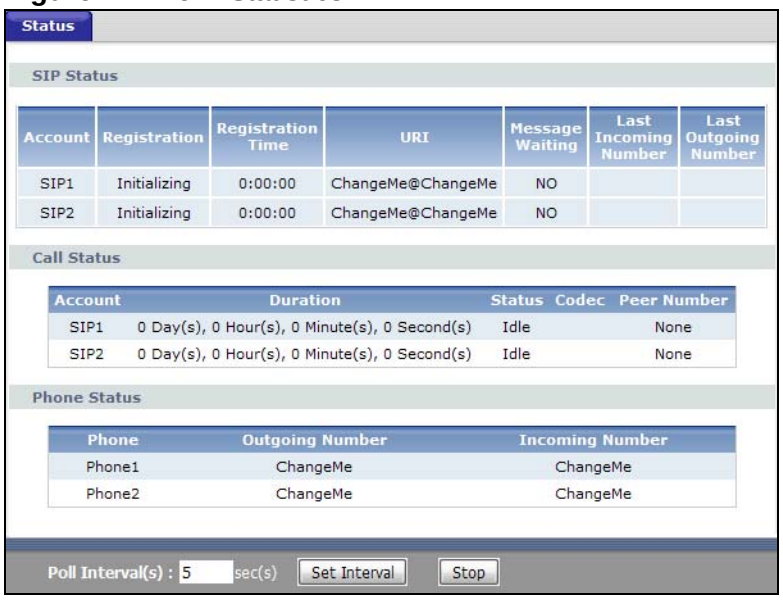
Table 7 Packet Statistics (continued)

LABEL	DESCRIPTION
Drops	This field applies to the WAN services and displays the number of packets that were received on this port and dropped.
Transmitted Bytes	This field displays the number of bytes transmitted on this port.
Pkts	This field displays the number of packets transmitted on this port.
Errs	This field displays the number of error packets transmitted on this port.
Drops	This field applies to the WAN services and displays the number of packets that were to be transmitted on this port but were dropped.
Poll Interval(s)	Type the time interval for the browser to refresh system statistics.
Set Interval	Click this to apply the new poll interval you entered in the **Poll Interval** field above.
Stop	Click this button to halt the refreshing of the system statistics.

4.5 VoIP Statistics

Click **Status > VoIP Statistics** to access this screen.

Figure 12 VoIP Statistics



Each field is described in the following table.

Table 8 VoIP Statistics

LABEL	DESCRIPTION
SIP Status	
Account	This column displays each SIP account in the ZyXEL Device.
Registration	This field displays the current registration status of the SIP account. You can change this in the **Status** screen. **Registered** - The SIP account is registered with a SIP server. **Register Fail** - The last time the ZyXEL Device tried to register the SIP account with the SIP server, the attempt failed. The ZyXEL Device automatically tries to register the SIP account when you turn on the ZyXEL Device or when you activate it. **Inactive** - The SIP account is not active. You can activate it in **VoIP > SIP > SIP Settings**.
Registration Time	This field displays the last time you successfully registered the SIP account. It displays **N/A** if you never successfully registered this account.
URI	This field displays the account number and service domain of the SIP account. You can change these in **VoIP > SIP > SIP Settings**.
Message Waiting	This field indicates whether or not there are any messages waiting for the SIP account.
Last Incoming Number	This field displays the last number that called the SIP account. It displays **N/A** if no number has ever dialed the SIP account.
Last Outgoing Number	This field displays the last number the SIP account called. It displays **N/A** if the SIP account has never dialed a number.
Call Status	
Account	This column displays each SIP account in the ZyXEL Device.
Duration	This field displays how long the current call has lasted.
Status	This field displays the current state of the phone call. **Idle** - There are no current VoIP calls, incoming calls or outgoing calls being made. **DIAL** - The callee's phone is ringing. **RING** - The phone is ringing for an incoming VoIP call. **Process** - There is a VoIP call in progress. **DISC** - The callee's line is busy, the callee hung up or your phone was left off the hook.
Codec	This field displays what voice codec is being used for a current VoIP call through a phone port.
Peer Number	This field displays the SIP number of the party that is currently engaged in a VoIP call through a phone port.
Phone Status	
Phone	This field displays each phone port in the ZyXEL Device.

Table 8 VoIP Statistics

LABEL	DESCRIPTION
Outgoing Number	This is the SIP number this phone port uses for making outgoing calls.
Incoming Number	This port will receive incoming calls for this SIP number.
Poll Interval(s)	Enter how often you want the ZyXEL Device to update this screen, and click **Set Interval**.
Set Interval	Click this to make the ZyXEL Device update the screen based on the amount of time you specified in **Poll Interval**.
Stop	Click this to make the ZyXEL Device stop updating the screen.

5

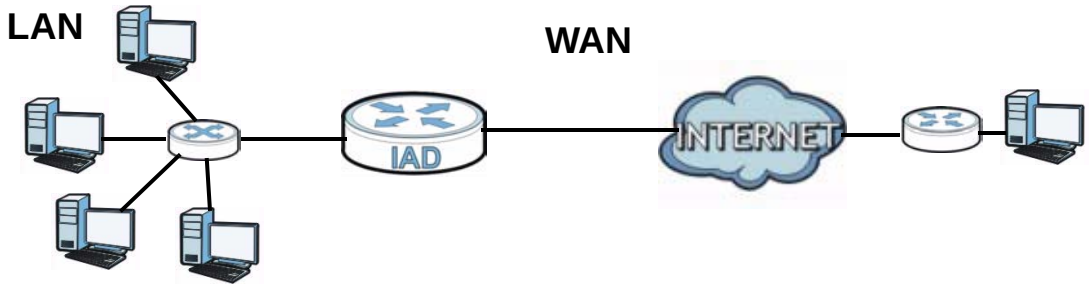
WAN Setup

5.1 Overview

This chapter discusses the ZyXEL Device's **WAN** screens. Use these screens to configure your ZyXEL Device for Internet access.

A WAN (Wide Area Network) connection is an outside connection to another network or the Internet. It connects your private networks, such as a LAN (Local Area Network) and other networks, so that a computer in one location can communicate with computers in other locations.

Figure 13 LAN and WAN



5.1.1 What You Can Do in this Chapter

- The **Layer 2 Interface** screen (Section 5.2 on page 99) lets you view, remove or add a layer-2 WAN interface.
- The **Internet Connection** screen (Section 5.3 on page 103) lets you view and configure the WAN settings on the ZyXEL Device for Internet access.

Table 9 WAN Setup Overview

LAYER-2 INTERFACE			INTERNET CONNECTION	
INTERFACE	**DSL LINK TYPE**	**CONNECTION MODE**	**WAN SERVICE TYPE**	**CONNECTION SETTINGS**
Ethernet		Default Mode VLAN MUX Mode (Note: This mode is not yet supported by the ZyXEL Device as of writing)	PPPoE	PPP user name and password, WAN IP address, DNS server and default gateway
			IPoE	WAN IP address, NAT, DNS server and default gateway
			Bridging	N/A
ATM	EoA	Default Mode VLAN MUX Mode (Note: This mode is not yet supported by the ZyXEL Device as of writing)	PPPoE	PPP user name and password, WAN IP address, DNS server and default gateway
			IPoE	WAN IP address, NAT, DNS server and default gateway
			Bridging	N/A
	PPPoA			PPP user name and password, WAN IP address, DNS server and default gateway
	IPoA			WAN IP address, NAT, DNS server and default gateway

5.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter.

Encapsulation Method

Encapsulation is used to include data from an upper layer protocol into a lower layer protocol. To set up a WAN connection to the Internet, you need to use the same encapsulation method used by your ISP (Internet Service Provider). If your ISP offers a dial-up Internet connection using PPPoE (PPP over Ethernet) or PPPoA, they should also provide a username and password (and service name) for user authentication.

WAN IP Address

The WAN IP address is an IP address for the ZyXEL Device, which makes it accessible from an outside network. It is used by the ZyXEL Device to communicate with other devices in other networks. It can be static (fixed) or

dynamically assigned by the ISP each time the ZyXEL Device tries to access the Internet.

If your ISP assigns you a static WAN IP address, they should also assign you the subnet mask and DNS server IP address(es).

ATM

Asynchronous Transfer Mode (ATM) is a LAN and WAN networking technology that provides high-speed data transfer. ATM uses fixed-size packets of information called cells. With ATM, a high QoS (Quality of Service) can be guaranteed. ATM uses a connection-oriented model and establishes a virtual circuit (VC) between two endpoints before the actual data exchange begins.

Finding Out More

- See Section 5.4 on page 113 for advanced technical information on WAN.
- See Chapter 3 on page 33 for WAN tutorials.

5.1.3 Before You Begin

You need to know your Internet access settings such as encapsulation and WAN IP address. Get this information from your ISP.

5.2 The Layer 2 Interface Screen

The ZyXEL Device must have a layer-2 interface to allow users to use the Ethernet WAN port or DSL port to access the Internet. The screen varies depending on the interface type you select.

Note: The ATM and Ethernet layer-2 interfaces cannot work at the same time.

Click **Network > WAN > Layer 2 Interface**. The following screen opens.

Figure 14 Network > WAN > Layer 2 Interface: Ethernet

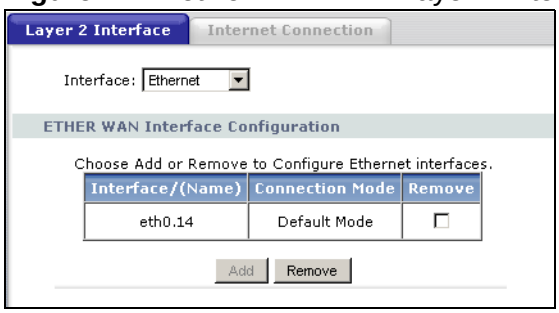
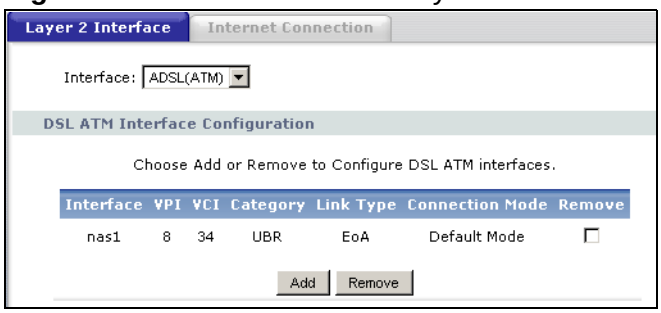


Figure 15 Network > WAN > Layer 2 Interface: ADSL ATM


Layer 2 Interface
Internet Connection
Interface: ADSL(ATM)
DSL ATM Interface Configuration
Choose Add or Remove to Configure DSL ATM interfaces.
Interface VPI VCI Category Link Type Connection Mode Remove
nas1 8 34 UBR EoA Default Mode
Add
Remove

The following table describes the fields in this screen. Some of the fields are not available for the Ethernet interface.

Table 10 Network > WAN > Layer 2 Interface

LABEL	DESCRIPTION
Interface	Select an interface for which you want to configure here. **ATM**: The ZyXEL Device uses the ADSL technology for data transmission over the DSL port. **Ethernet**: The ZyXEL Device transmits data over the Ethernet WAN port. Select this if you have a DSL router or modem in your network already.
Interface/ (Name)	This is the name of the interface.
VPI	This is the Virtual Path Identifier (VPI).
VCI	This is the Virtual Channel Identifier (VCI).
Category	This is the ATM traffic class.
Link Type	This is the DSL link type of the ATM layer-2 interface.
Connection Mode	This displays the connection mode of the layer-2 interface.
Remove	Check this and click the **Remove** button to delete this interface from the ZyXEL Device. A window displays asking you to confirm that you want to delete the interface. Note: You cannot remove the layer-2 interface when a WAN service is associated with it.

Table 10 Network > WAN > Layer 2 Interface

LABEL	DESCRIPTION
Add	Click this button to create a new layer-2 interface.
Remove	Check **Remove** and click this to delete this interface from the ZyXEL Device. A window displays asking you to confirm that you want to delete the interface.

5.2.1 Layer 2 Interface Configuration

Use this screen to create a new layer-2 interface. At the time of writing, you can configure only one Ethernet layer-2 interface on the ZyXEL Device. However, you can create multiple ATM layer-2 interfaces. The screen varies depending on the interface type you selected in the previous section.

Click **Add** in the **Network > WAN > Layer 2 Interface** screen to open the following.

Figure 16 Network > WAN > Layer 2 Interface: Ethernet WAN Interface Configuration

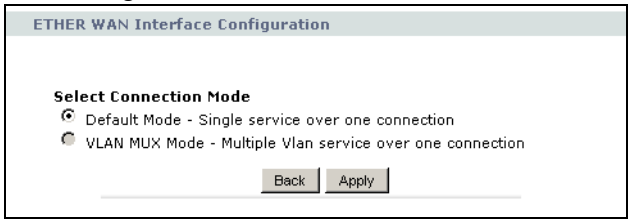
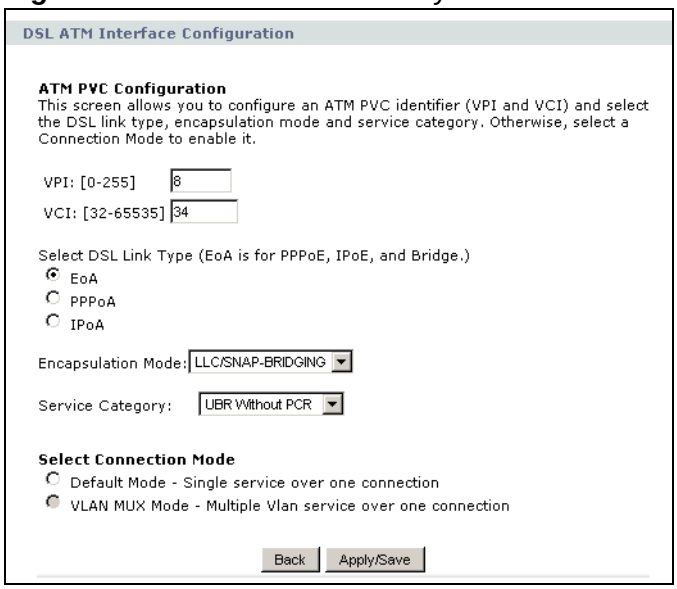

ETHER WAN Interface Configuration
Select Connection Mode
Default Mode - Single service over one connection
VLAN MUX Mode - Multiple Vlan service over one connection
Back
Apply

Figure 17 Network > WAN > Layer 2 Interface: DSL ATM Interface Configuration


DSL ATM Interface Configuration
ATM PVC Configuration
This screen allows you to configure an ATM PVC identifier (VPI and VCI) and select the DSL link type, encapsulation mode and service category. Otherwise, select a Connection Mode to enable it.
VPI: [0-255] 8
VCI: [32-65535] 34
Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)
EoA
PPPoA
IPoA
Encapsulation Mode: LLC/SNAP-BRIDGING
Service Category: UBR Without PCR
Select Connection Mode
Default Mode - Single service over one connection
VLAN MUX Mode - Multiple Vlan service over one connection
Back
Apply/Save

Note: VLAN MUX Mode is not supported by the ZyXEL Device as of writing.

The following table describes the fields in this screen.

Table 11 Network > WAN > Layer 2 Interface: Configuration

LABEL	DESCRIPTION
ATM PVC Configuration	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. This section is available only when you configure a DSL ATM layer-2 interface.
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
Select DSL Link Type	Select **EoA** (Ethernet over ATM) to have an Ethernet header in the packet, so that you can have multiple services/connections over one PVC. You can set each connection to have its own MAC address or all connections share one MAC address but use different VLAN IDs for different services. **EoA** supports IPoE, PPPoE and RFC1483/2684 bridging encapsulation methods. Select **PPPoA** (PPP over ATM) to allow just one PPPoA connection over a PVC. Select **IPoA** (IP over ATM) to allow just one RFC 1483/2684 routing connection over a PVC.
Encapsulation Mode	Select the method of multiplexing used by your ISP from the drop-down list. Choices are: • **VC/MUX**: In VC multiplexing, each protocol is carried on a single ATM virtual circuit (VC). To transport multiple protocols, the ZyXEL Device needs separate VCs. There is a binding between a VC and the type of the network protocol carried on the VC. This reduces payload overhead since there is no need to carry protocol information in each Protocol Data Unit (PDU) payload. • **LLC/ENCAPSULATION**: More than one protocol can be carried over the same VC. This is available only when you select **PPPoA** in the **Select DSL Link Type** field. • **LLC/SNAP-ROUTING**: In LCC encapsulation, an IEEE 802.2 Logical Link Control (LLC) header is prefixed to each routed PDU to identify the PDUs. The LCC header can be followed by an IEEE 802.1a SubNetwork Attachment Point (SNAP) header. This is available only when you select **IPoA** in the **Select DSL Link Type** field. • **LLC/SNAP-BRIDGING**: In LCC encapsulation, bridged PDUs are encapsulated by identifying the type of the bridged media in the SNAP header. This is available only when you select **EoA** in the **Select DSL Link Type** field.
Service Category	Select **UBR Without PCR** for applications that are non-time sensitive, such as e-mail. Select **CBR** (Constant Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select **Realtime VBR** (real-time Variable Bit Rate) for applications with bursty connections that require closely controlled delay and delay variation. Select **Non Realtime VBR** (non real-time Variable Bit Rate) for connections that do not require closely controlled delay and delay variation.

Table 11 Network > WAN > Layer 2 Interface: Configuration (continued)

LABEL	DESCRIPTION
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here. This field is not available when you select **UBR Without PCR**.
Sustainable Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec. This field is available only when you select **Non Realtime VBR** or **Realtime VBR**.
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535. This field is available only when you select **Non Realtime VBR** or **Realtime VBR**.
Select Connection Mode	Select **Default Mode**. This allows only one WAN service over a single virtual circuit. **VLAN MUX Mode** is not supported by the ZyXEL Device as of writing. This field is not available if you select **PPPoA** or **IPoA** in the **DSL Link Type** field.
Back	Click this button to return to the previous screen without saving any changes.
Apply/Save	Click this button to save your changes and go back to the previous screen.

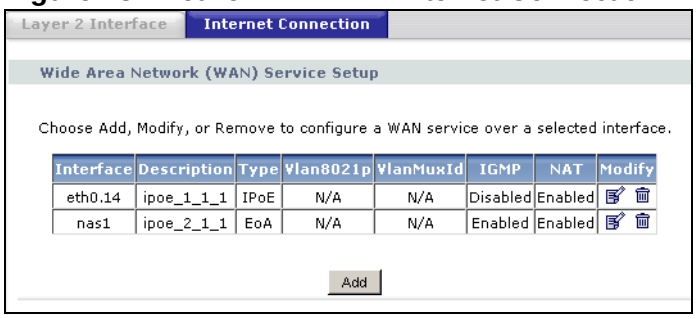
5.3 The Internet Connection Screen

Use this screen to change your ZyXEL Device's WAN settings. Click **Network > WAN > Internet Connection**. The summary table shows you the configured WAN services (connections) on the ZyXEL Device.

Note: To use NAT or IGMP proxy in the ZyXEL Device, you need to configure a WAN connection with PPPoE or IPoE.

Note: You can configure up to eight (8) WAN services for each interface.

Figure 18 Network > WAN > Internet Connection


Layer 2 Interface
Internet Connection
Wide Area Network (WAN) Service Setup
Choose Add, Modify, or Remove to configure a WAN service over a selected interface.
Interface Description Type Vlan8021p VlanMuxId IGMP NAT Modify
eth0.14 ipoe_1_1_1 IPoE N/A N/A Disabled Enabled
nas1 ipoe_2_1_1 EoA N/A N/A Enabled Enabled
Add

The following table describes the labels in this screen.

Table 12 Network > WAN > Internet Connection

LABEL	DESCRIPTION
Interface	This shows the name of the interface used by this connection. A default name **nas** followed by a number (for example, **nas1**) indicates the DSL interface. The name **eth0.14** indicates the default Ethernet WAN interface (the physical Ethernet WAN port). The number after the dot (**.**) represents the VLAN ID number assigned to traffic sent through this connection.
Description	This is the service name of this connection. 1 and 2 or 0 and 1 are the default VPI and VCI numbers. The last number represents the index number of connections over the same PVC or the VLAN ID number assigned to traffic sent through this connection.
Type	This shows the method of encapsulation used by this connection.
Vlan8021p	This indicates the 802.1P priority level assigned to traffic sent through this connection. This displays **N/A** when there is no priority level assigned.
VlanMuxId	This indicates the VLAN ID number assigned to traffic sent through this connection. This displays **N/A** when there is no VLAN ID number assigned.
IGMP	This shows whether IGMP (Internet Group Multicast Protocol) is activated or not for this connection. IGMP is not available when the connection uses the bridging service.
NAT	This shows whether NAT is activated or not for this interface. NAT is not available when the connection uses the bridging service.
Modify	Click the **Edit** icon to configure the WAN connection. Click the **Remove** icon to delete the WAN connection.
Add	Click **Add** to create a new connection.

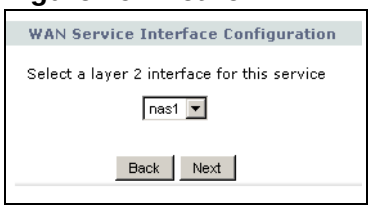
5.3.1 WAN Connection Configuration

Click the **Edit** or **Add** button in the **Network > WAN > Internet Connection** screen to configure a WAN connection.

5.3.1.1 WAN Interface

This screen displays when you add a new WAN connection.

Figure 19 Network > WAN > Internet Connection: Adding a WAN Interface



The following table describes the labels in this screen.

Table 13 Network > WAN > Internet Connection: Adding a WAN Interface

LABEL	DESCRIPTION
Select a layer 2 interface for this service	Select an ATM interface. The ATM interface name starts with **nas** followed by a number (for example, **nas1**). This uses the DSL port as the WAN port and ADSL technology for data transmission. Select **eth0.14** if you want to use the Ethernet WAN port as the WAN port.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

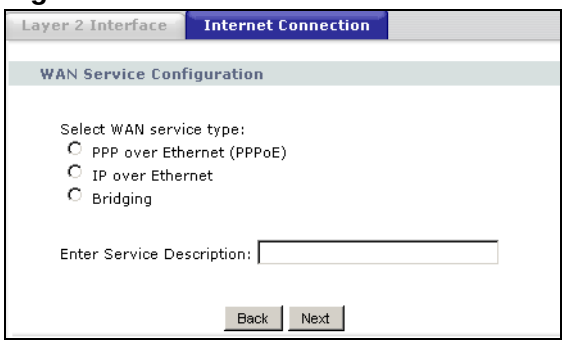
5.3.1.2 WAN Service Type

Use this screen to select your WAN service type. Click **Next** in the **Network > WAN > Internet Connection** screen. There are two possible screens as follows.

This screen shows for the Ethernet WAN interface by default; for DSL WAN interface, this shows when you select **EoA** as the **DSL Link Type** field in the

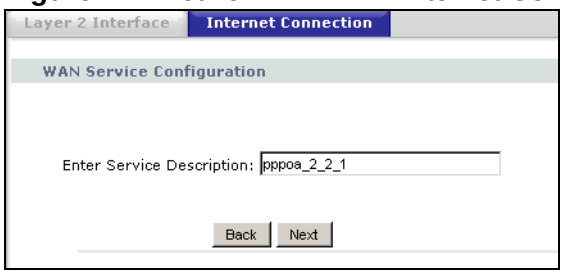
Network > WAN > Layer 2 Interface: DSL ATM Interface Configuration screen.

Figure 20 Network > WAN > Internet Connection: Service Type - EoA



On the other hand, the following screen shows if you select **PPPoA** or **IPoA** as the **DSL Link Type** field in the **Network > WAN > Layer 2 Interface: DSL ATM Interface Configuration** screen. You only need to configure the **Enter Service Description** field in this screen as follows.

Figure 21 Network > WAN > Internet Connection: Service Type - PPPoA or IPoA



The following table describes the labels in this screen.

Table 14 Network > WAN > Internet Connection: Service Type

LABEL	DESCRIPTION
Select WAN service type	Select the method of encapsulation used by your ISP. Choices are **PPP over Ethernet (PPPoE)**, **IP over Ethernet** and **Bridging**: • **PPP over Ethernet (PPPoE)** - PPPoE (Point to Point Protocol over Ethernet) provides access control and billing functionality in a manner similar to dial-up services using PPP. Select this if you have a username and password for Internet access. • **IP over Ethernet** - In this type of Internet connection, IP packets are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment. • **Bridging** - With bridging the ZyXEL Device has a static IP address for the connection. The ZyXEL Device passes traffic through to another device (a computer or router for example) that handles authenticating with the ISP. Note: This field does not show for a PPPoA or IPoA service type.
Enter Service Description	Specify a name for this connection or use the automatically generated one. You can type up to 31 characters, using alphanumeric characters, '_' and '-' (no spaces allowed).
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

5.3.1.3 WAN IP Address, NAT and IGMP Proxy

Click **Next** in the **Network > WAN > Internet Connection: Service Type** screen. There are three possible screens as follows.

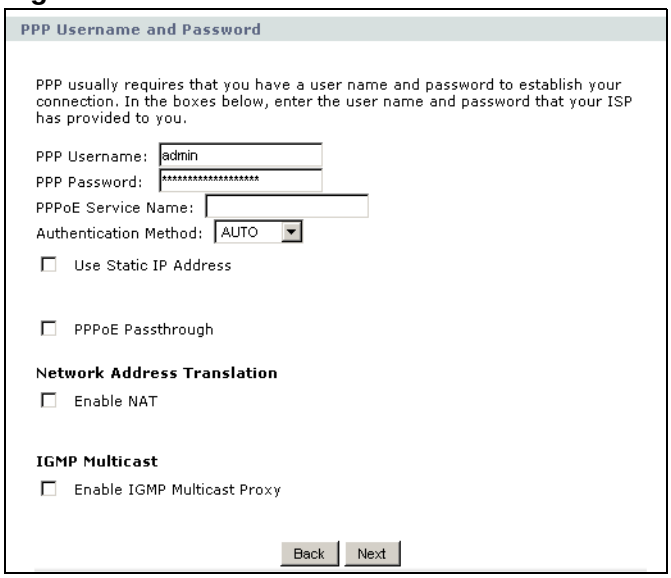
PPPoE or PPPoA

This screen displays when you select **PPP over Ethernet (PPPoE)** in the previous section for an Ethernet WAN interface. For the DSL WAN interface, this shows:

- If you set the **DSL Link Type** field in the **Network > WAN > Layer 2 Interface** screen to **EoA** and select **PPP over Ethernet (PPPoE)** in the previous section.
- If you set the **DSL Link Type** field in the **Network > WAN > Layer 2 Interface** screen to **PPPoA** and click **Next** in the previous section.

Note: Make sure you have the correct account information from your ISP or network administrator when configuring this screen.

Figure 22 Network > WAN > Internet Connection: PPPoE or PPPoA


PPP Username and Password
PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.
PPP Username:
admin
PPP Password:
PPPoE Service Name:
Authentication Method:
AUTO
Use Static IP Address
PPPoE Passthrough
Network Address Translation
Enable NAT
IGMP Multicast
Enable IGMP Multicast Proxy
Back
Next

The following table describes the labels in this screen.

Table 15 Network > WAN > Internet Connection: PPPoE or PPPoA

LABEL	DESCRIPTION
PPP User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
PPP Password	Enter the password associated with the user name above.
PPPoE Service Name	Type the name of your PPPoE service here. This field is not available for a PPPoA connection (DSL WAN interface).
Authentication Method	The ZyXEL Device supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is readily available on more platforms. Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: **AUTO** - Your ZyXEL Device accepts either CHAP or PAP when requested by this remote node. **CHAP** - Your ZyXEL Device accepts CHAP only. **PAP** - Your ZyXEL Device accepts PAP only. **MSCHAP** - Your ZyXEL Device accepts MSCHAP only. MS-CHAP is the Microsoft version of the CHAP.
Use Static IP Address	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select this if you do not have a dynamic IP address.

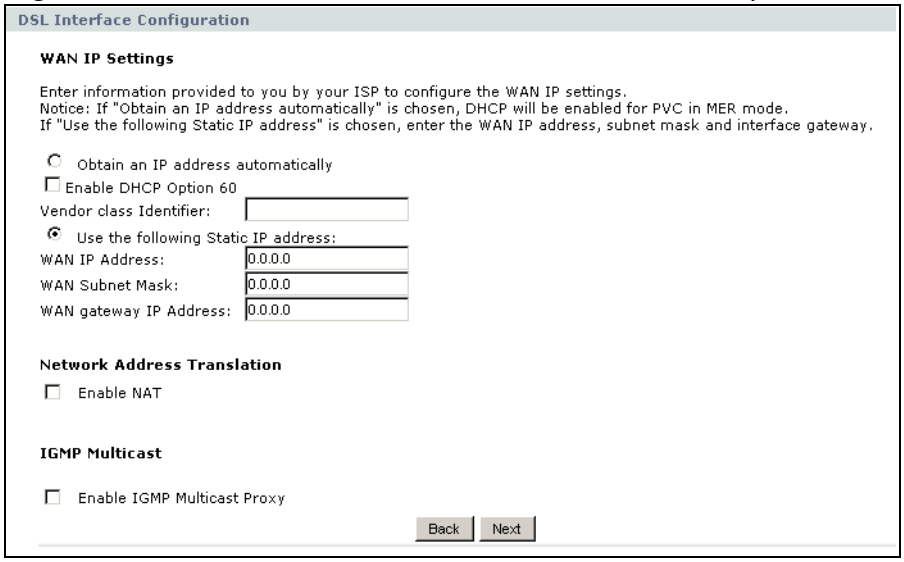
Table 15 Network > WAN > Internet Connection: PPPoE or PPPoA

LABEL	DESCRIPTION
IP Address	Enter the static IP address provided by your ISP.
PPPoE Passthrough	This field is available when you select PPPoE encapsulation. In addition to the ZyXEL Device's built-in PPPoE client, you can enable PPPoE pass through to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP via the ZyXEL Device. Each host can have a separate account and a public WAN IP address. PPPoE pass through is an alternative to NAT for application where NAT is not appropriate. Disable PPPoE pass through if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.
Enable NAT	Select this option to enable NAT on the ZyXEL Device.
Enable IGMP Multicast Proxy	Select this check box to have the ZyXEL Device act as an IGMP proxy on this connection. This allows the ZyXEL Device to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

IPoE

This screen displays when you select **IP over Ethernet** in the previous section for an Ethernet WAN interface. This screen does not show for the DSL WAN interface.

Figure 23 Network > WAN > Internet Connection: IPoE (Ethernet WAN Interface)


DSL Interface Configuration
WAN IP Settings
Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in MER mode.
If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway.
Obtain an IP address automatically
Enable DHCP Option 60
Vendor class Identifier:
Use the following Static IP address:
WAN IP Address: 0.0.0.0
WAN Subnet Mask: 0.0.0.0
WAN gateway IP Address: 0.0.0.0
Network Address Translation
Enable NAT
IGMP Multicast
Enable IGMP Multicast Proxy
Back
Next

The following table describes the labels in this screen.

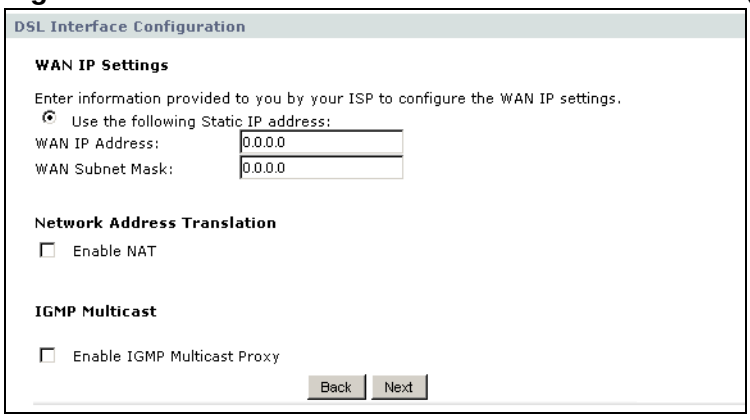
Table 16 Network > WAN > Internet Connection: IPoE (Ethernet WAN Interface)

LABEL	DESCRIPTION
Obtain an IP address automatically	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select this if you do not have a static IP address.
Enable DHCP Option 60	Select this to identify the vendor and functionality of the ZyXEL Device in DHCP requests that the ZyXEL Device sends to a DHCP server when getting a WAN IP address.
Vendor Class Identifier	Enter the Vendor Class Identifier (Option 60), such as the type of the hardware or firmware.
Use the following Static IP address	Select this if you have a static IP address.
WAN IP Address	Enter the static IP address provided by your ISP.
WAN Subnet Mask	Enter the subnet mask provided by your ISP.
WAN gateway IP Address	Enter the gateway IP address provided by your ISP.
Enable NAT	Select this option to enable NAT on the ZyXEL Device.
Enable IGMP Multicast Proxy	Select this check box to have the ZyXEL Device act as an IGMP proxy on this connection. This allows the ZyXEL Device to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

IPoA

This shows if you set the **DSL Link Type** field in the **Network > WAN > Layer 2 Interface** screen to **IPoA**. This screen does not show for the Ethernet WAN interface.

Figure 24 Network > WAN > Internet Connection: IPoA (DSL WAN Interface)



The following table describes the labels in this screen.

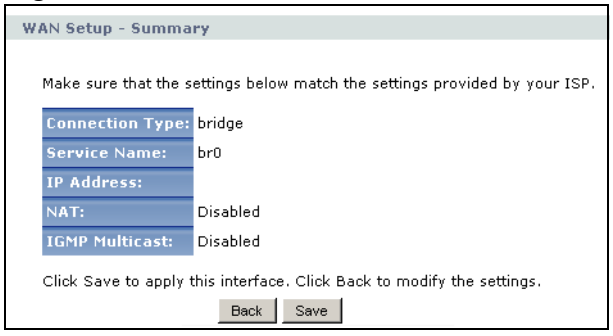
Table 17 Network > WAN > Internet Connection: IPoA (DSL WAN Interface)

LABEL	DESCRIPTION
WAN IP Address	Enter the static IP address provided by your ISP.
WAN Subnet Mask	Enter the subnet mask provided by your ISP.
Enable NAT	Select this option to enable NAT on the ZyXEL Device.
Enable IGMP Multicast Proxy	Select this check box to have the ZyXEL Device act as an IGMP proxy on this connection. This allows the ZyXEL Device to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

Bridging

This screen displays when you select **Bridging** in the previous section for an Ethernet WAN interface. For the DSL WAN interface, this shows if you set the **DSL Link Type** field in the **Network > WAN > Layer 2 Interface** screen to **EoA** and select **Bridging** in the previous section.

Figure 25 Network > WAN > Internet Connection: Bridging


WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
Connection Type: bridge
Service Name: br0
IP Address:
NAT: Disabled
IGMP Multicast: Disabled
Click Save to apply this interface. Click Back to modify the settings.
Back
Save

The following table describes the labels in this screen.

Table 18 Network > WAN > Internet Connection: Bridging

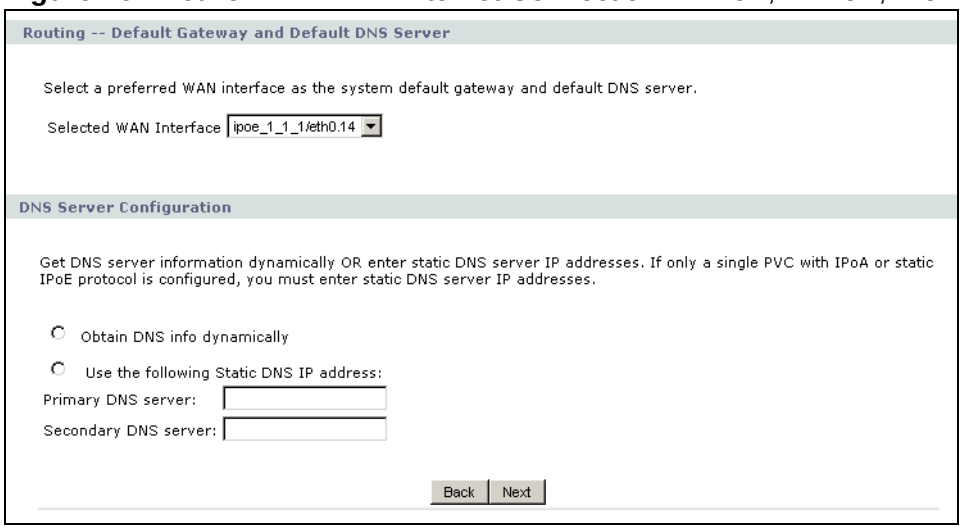
LABEL	DESCRIPTION
Connection Type	This is the encapsulation method used by this connection.
Service Name	This is the name of the service.
IP Address	This shows whether the WAN IP address is assigned by the ISP, manually configured or not configurable.
NAT	This shows whether NAT is active or not for this connection.
IGMP Multicast	This shows whether IGMP multicasting is active or not for this connection.
Back	Click this button to return to the previous screen.
Save	Click this button to save your changes.

5.3.1.4 Routing and DNS Server

Click **Next** in the screens shown in Section 5.3.1.3 on page 107. This screen shows for both Ethernet and DSL WAN interfaces except when you select **Bridging** as a service type.

Note: If you configure only one IPoA connection using the ATM interface on the ZyXEL Device, you must enter the static DNS server address.

Figure 26 Network > WAN > Internet Connection: PPPoE, PPPoA, IPoE or IPoA


Routing -- Default Gateway and Default DNS Server
Select a preferred WAN interface as the system default gateway and default DNS server.
Selected WAN Interface
ipoe_1_1_1/eth0.14
DNS Server Configuration
Get DNS server information dynamically OR enter static DNS server IP addresses. If only a single PVC with IPoA or static IPoE protocol is configured, you must enter static DNS server IP addresses.
Obtain DNS info dynamically
Use the following Static DNS IP address:
Primary DNS server:
Secondary DNS server:
Back
Next

The following table describes the labels in this screen.

Table 19 Network > WAN > Internet Connection: PPPoE, PPPoA, IPoE or IPoA

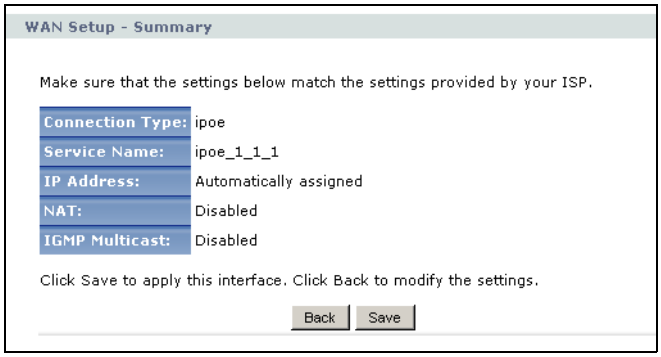
LABEL	DESCRIPTION
Selected WAN Interfaces	Select a WAN interface through which you want to obtain a system default server and DNS server.
Obtain DNS info dynamically	Select this to have the ZyXEL Device use the DNS server addresses assigned by your ISP.
Use the following Static DNS IP address	Select this to have the ZyXEL Device use the DNS server addresses you configure manually.
Primary DNS server	Enter the first DNS server address assigned by the ISP.
Secondary DNS server	Enter the second DNS server address assigned by the ISP.
Back	Click this button to return to the previous screen.
Next	Click this button to continue.

5.3.1.5 Configuration Summary

Click **Next** in the previous section to open this read-only screen that shows the current WAN connection settings.

This screens shows for all WAN interface and service types as well as all DSL link types as the last step in the WAN setup process.

Figure 27 Network > WAN > Internet Connection: WAN Configuration Summary


WAN Setup - Summary
Make sure that the settings below match the settings provided by your ISP.
Connection Type: ipoe
Service Name: ipoe_1_1_1
IP Address: Automatically assigned
NAT: Disabled
IGMP Multicast: Disabled
Click Save to apply this interface. Click Back to modify the settings.
Back
Save

The following table describes the labels in this screen.

Table 20 WAN Configuration: Configuration Summary

LABEL	DESCRIPTION
Connection Type	This is the encapsulation method used by this connection.
Service Name	This is the name of the service.
IP Address	This shows whether the WAN IP address is assigned by the ISP, manually configured or not configurable.
NAT	This shows whether NAT is active or not for this connection.
IGMP Multicast	This shows whether IGMP multicasting is active or not for this connection.
Back	Click this button to return to the previous screen.
Apply/Save	Click this button to save your changes.

5.4 Technical Reference

The following section contains additional technical information about the ZyXEL Device features described in this chapter.

Encapsulation

Be sure to use the encapsulation method required by your ISP. The ZyXEL Device can work in bridge mode or routing mode. When the ZyXEL Device is in routing mode, it supports the following methods.

IP over Ethernet

IP over Ethernet (IPoE) is an alternative to PPPoE. IP packets are being delivered across an Ethernet network, without using PPP encapsulation. They are routed

between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment. For instance, it encapsulates routed Ethernet frames into bridged Ethernet cells.

PPP over Ethernet

Point-to-Point Protocol over Ethernet (PPPoE) provides access control and billing functionality in a manner similar to dial-up services using PPP. PPPoE is an IETF standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example RADIUS).

One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the ZyXEL Device (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the ZyXEL Device does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

PPPoA

PPPoA stands for Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). A PPPoA connection functions like a dial-up Internet connection. The ZyXEL Device encapsulates the PPP session based on RFC1483 and sends it through an ATM PVC (Permanent Virtual Circuit) to the Internet Service Provider's (ISP) DSLAM (digital access multiplexer). Please refer to RFC 2364 for more information on PPPoA. Refer to RFC 1661 for more information on PPP.

RFC 1483

RFC 1483 describes two methods for Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5). The first method allows multiplexing of multiple protocols over a single ATM virtual circuit (LLC-based multiplexing) and the second method assumes that each protocol is carried over a separate ATM virtual circuit (VC-based multiplexing). Please refer to RFC 1483 for more detailed information.

Multiplexing

There are two conventions to identify what protocols the virtual circuit (VC) is carrying. Be sure to use the multiplexing method required by your ISP.

VC-based Multiplexing

In this case, by prior mutual agreement, each protocol is assigned to a specific virtual circuit; for example, VC1 carries IP, etc. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.

LLC-based Multiplexing

In this case one VC carries multiple protocols with protocol identifying information being contained in each packet header. Despite the extra bandwidth and processing overhead, this method may be advantageous if it is not practical to have a separate VC for each carried protocol, for example, if charging heavily depends on the number of simultaneous VCs.

Traffic Shaping

Traffic Shaping is an agreement between the carrier and the subscriber to regulate the average rate and fluctuations of data transmission over an ATM network. This agreement helps eliminate congestion, which is important for transmission of real time data such as audio and video connections.

Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. This parameter may be lower (but not higher) than the maximum line speed. 1 ATM cell is 53 bytes (424 bits), so a maximum speed of 832Kbps gives a maximum PCR of 1962 cells/sec. This rate is not guaranteed because it is dependent on the line speed.

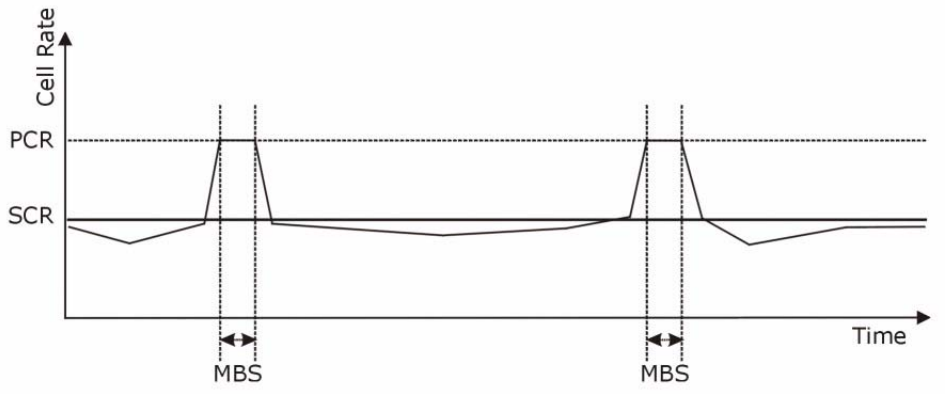
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

Maximum Burst Size (MBS) is the maximum number of cells that can be sent at the PCR. After MBS is reached, cell rates fall below SCR until cell rate averages to the SCR again. At this time, more cells (up to the MBS) can be sent at the PCR again.

If the PCR, SCR or MBS is set to the default of "0", the system will assign a maximum value that correlates to your upstream line rate.

The following figure illustrates the relationship between PCR, SCR and MBS.

Figure 28 Example of Traffic Shaping



ATM Traffic Classes

These are the basic ATM traffic classes defined by the ATM Forum Traffic Management 4.0 Specification.

Constant Bit Rate (CBR)

Constant Bit Rate (CBR) provides fixed bandwidth that is always available even if no data is being sent. CBR traffic is generally time-sensitive (doesn't tolerate delay). CBR is used for connections that continuously require a specific amount of bandwidth. A PCR is specified and if traffic exceeds this rate, cells may be dropped. Examples of connections that need CBR would be high-resolution video and voice.

Variable Bit Rate (VBR)

The Variable Bit Rate (VBR) ATM traffic class is used with bursty connections. Connections that use the Variable Bit Rate (VBR) traffic class can be grouped into real time (VBR-RT) or non-real time (VBR-nRT) connections.

The VBR-RT (real-time Variable Bit Rate) type is used with bursty connections that require closely controlled delay and delay variation. It also provides a fixed amount of bandwidth (a PCR is specified) but is only available when data is being sent. An example of an VBR-RT connection would be video conferencing. Video conferencing requires real-time data transfers and the bandwidth requirement varies in proportion to the video image's changing dynamics.

The VBR-nRT (non real-time Variable Bit Rate) type is used with bursty connections that do not require closely controlled delay and delay variation. It is commonly used for "bursty" traffic typical on LANs. PCR and MBS define the burst levels, SCR defines the minimum level. An example of an VBR-nRT connection would be non-time sensitive data file transfers.

Unspecified Bit Rate (UBR)

The Unspecified Bit Rate (UBR) ATM traffic class is for bursty data transfers. However, UBR doesn't guarantee any bandwidth and only delivers traffic when the network has spare bandwidth. An example application is background file transfer.

IP Address Assignment

A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed; the ISP assigns you a different one each time. The Single User Account feature can be enabled or disabled if you have either a dynamic or static IP. However the encapsulation method assigned influences your choices for IP address and default gateway.

Introduction to VLANs

A Virtual Local Area Network (VLAN) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.

In Multi-Tenant Unit (MTU) applications, VLAN is vital in providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN, thus a user will not see the printers and hard disks of another user in the same building.

VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

Introduction to IEEE 802.1Q Tagged VLAN

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the switch on which they were created. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID (Tag Protocol Identifier), residing within the type/ length field of the Ethernet frame) and two bytes of TCI (Tag Control Information), starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then

that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

TPID	User Priority	CFI	VLAN ID
2 Bytes	3 Bits	1 Bit	12 Bits

Multicast

IP packets are transmitted in either one of two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

At start up, the ZyXEL Device queries all directly connected networks to gather group membership. After that, the ZyXEL Device periodically updates this information.

DNS Server Address Assignment

Use Domain Name System (DNS) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of www.zyxel.com is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

The ZyXEL Device can get the DNS server addresses in the following ways.

1. The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.

2. If your ISP dynamically assigns the DNS server IP addresses (along with the ZyXEL Device's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

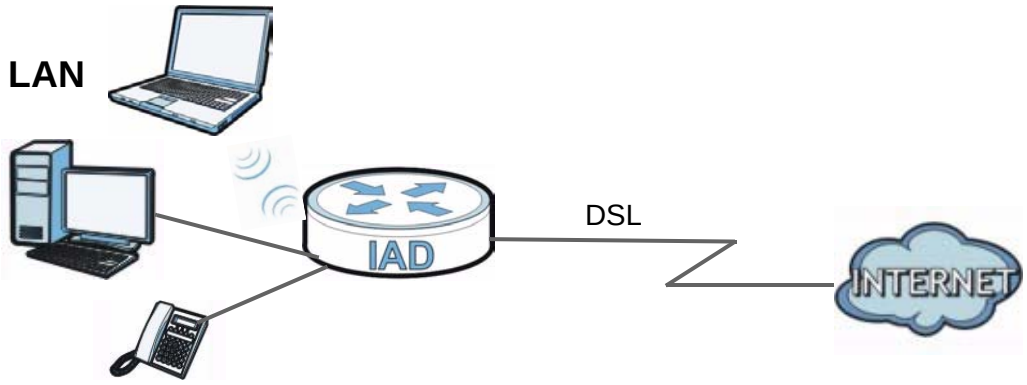
6

LAN Setup

6.1 Overview

A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is usually located in one immediate area such as a building or floor of a building.

The LAN screens can help you configure a LAN DHCP server and manage IP addresses.



- See Section 6.5 on page 126 for more information on LANs.
- See Appendix A on page 293 for more information on IP addresses and subnetting.

6.1.1 What You Can Do in this Chapter

- Use the **IP** screen (Section 6.2 on page 122) to set the LAN IP address and subnet mask of your ZyXEL device.
- Use the **DHCP Server** screen (Section 6.3 on page 123) to configure the DNS server information that the ZyXEL Device sends to the DHCP client devices on the LAN.
- Use the **Client List** screen (Section 6.4 on page 124) to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.

6.1.2 What You Need To Know

The following terms and concepts may help as you read this chapter.

IP Address

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number. This is known as an Internet Protocol address.

Subnet Mask

The subnet mask specifies the network number portion of an IP address. Your ZyXEL Device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the ZyXEL Device unless you are instructed to do otherwise.

DHCP

DHCP (Dynamic Host Configuration Protocol) allows clients to obtain TCP/IP configuration at start-up from a server. This ZyXEL Device has a built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

DNS

DNS (Domain Name System) maps a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The DNS server addresses you enter when you set up DHCP are passed to the client machines along with the assigned IP address and subnet mask.

6.1.3 Before You Begin

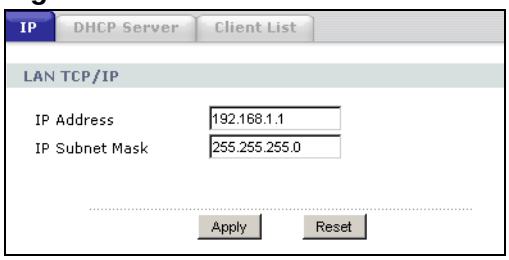
Find out the MAC addresses of your network devices if you intend to add them to the DHCP Client List screen.

6.2 The IP Screen

Click **Network > LAN** to open the **IP** screen. See Section 6.1 on page 121 for background information. Use this screen to set the Local Area Network IP address

and subnet mask of your ZyXEL Device and configure the DNS server information that the ZyXEL Device sends to the DHCP client devices on the LAN.

Figure 29 Network > LAN > IP



The following table describes the fields in this screen.

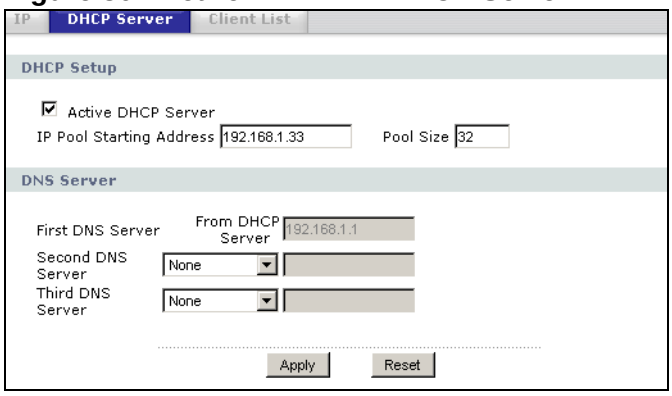
Table 21 Network > LAN > IP

LABEL	DESCRIPTION
IP Address	Enter the LAN IP address you want to assign to your ZyXEL Device in dotted decimal notation, for example, 192.168.1.1 (factory default).
IP Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your ZyXEL Device automatically computes the subnet mask based on the IP address you enter, so do not change this field unless you are instructed to do so.
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to begin configuring this screen afresh.

6.3 DHCP Server Screen

Use this screen to configure the DNS server information that the ZyXEL Device sends to the DHCP client devices on the LAN.

Figure 30 Network > LAN > DHCP Server



The following table describes the labels in this screen.

Table 22 Network > LAN > DHCP Server

LABEL	DESCRIPTION
DHCP Setup	
Active DHCP Server	Select this to have your ZyXEL Device assign IP addresses, an IP default gateway and DNS servers to LAN computers and other devices that are DHCP clients. If you do not check this, the DHCP server will be disabled. You need to manually configure the IP addresses of the computers and other devices on your LAN. When DHCP is used, the following fields need to be set.
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.
DNS Server	
First DNS Server Second DNS Server Third DNS Server	Select **From ISP** if your ISP dynamically assigns DNS server information (and the ZyXEL Device's WAN IP address). Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. You must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
Apply	Click this to save the changes.
Reset	Click this to begin configuring this screen afresh.

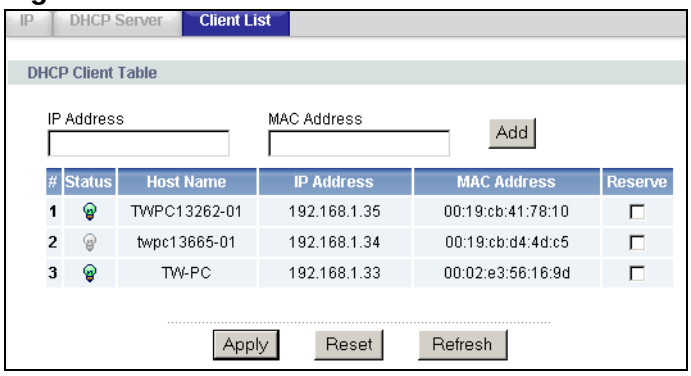
6.4 The Client List Screen

Use this table to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

Click **Network > LAN > Client List** to open the following screen. Use this screen to change your ZyXEL Device's static DHCP settings.

Figure 31 Network > LAN > Client List



The following table describes the labels in this screen.

Table 23 Network > LAN > Client List

LABEL	DESCRIPTION
IP Address	Enter the IP address that you want to assign to the computer on your LAN with the MAC address that you will also specify.
MAC Address	Enter the MAC address of a computer on your LAN.
Add	Click **Add** to add a static DHCP entry.
#	This is the index number of the static IP table entry (row).
Status	This field displays whether the client is connected to the ZyXEL Device.
Host Name	This field displays the computer host name.
IP Address	This field displays the IP address relative to the # field listed above.
MAC Address	The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation). A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
Reserve	Select the check box in the heading row to automatically select all check boxes or select the check box(es) in each entry to have the ZyXEL Device always assign the selected entry(ies)'s IP address(es) to the corresponding MAC address(es) (and host name(s)). You can select up to 128 entries in this table.
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to begin configuring this screen afresh.
Refresh	Click this to reload the DHCP table.

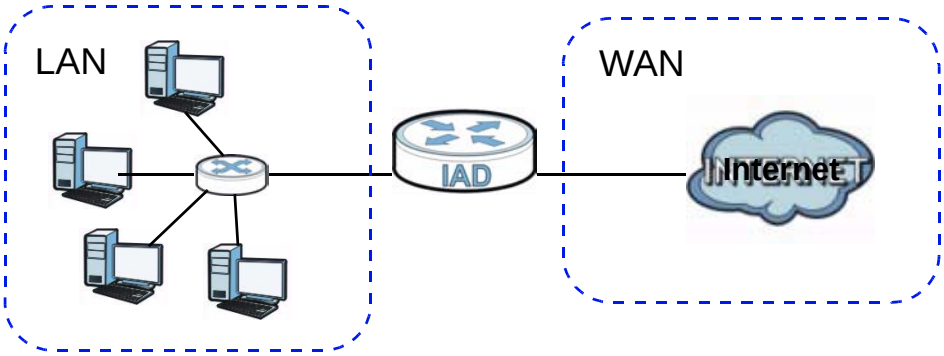
6.5 Technical Reference

This section provides some technical background information about the topics covered in this chapter.

LANs, WANs and the ZyXEL Device

The actual physical connection determines whether the ZyXEL Device ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

Figure 32 LAN and WAN IP Addresses



DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the ZyXEL Device as a DHCP server or disable it. When configured as a server, the ZyXEL Device provides the TCP/IP configuration for the clients. If you turn DHCP service off, you must have another DHCP server on your LAN, or else the computer must be manually configured.

IP Pool Setup

The ZyXEL Device is pre-configured with a pool of IP addresses for the DHCP clients (DHCP Pool). See the product specifications in the appendices. Do not assign static IP addresses from the DHCP pool to your LAN computers.

LAN TCP/IP

The ZyXEL Device has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the ZyXEL Device. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your ZyXEL Device, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your ZyXEL Device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the ZyXEL Device unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet, for example, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger

organization, you should consult your network administrator for the appropriate IP addresses.

Note: Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, “Address Allocation for Private Internets” and RFC 1466, “Guidelines for Management of IP Address Space”.

7

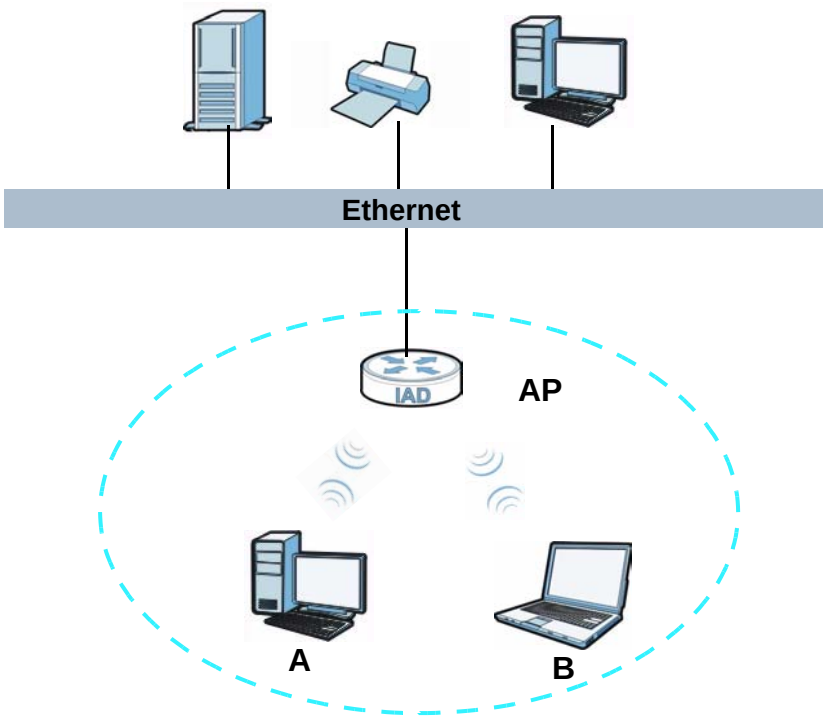
Wireless LAN

7.1 Overview

This chapter describes the ZyXEL Device's **Network > Wireless LAN** screens. Use these screens to set up your ZyXEL Device's wireless connection.

The blue circle marks a wireless LAN in the following figure. Wireless clients (A and B) connect to an access point (AP) to access other devices (such as the printer) or the Internet. Your ZyXEL Device works as an AP when you install a compatible WLAN card.

Figure 33 Example of a Wireless Network



7.1.1 What You Can Do in this Chapter

- Use the **General** screen (see Section 7.2 on page 133) to turn the wireless connection on or off, create multiple SSIDs and make other configuration changes.

- Use the **Security** screens (see Section 7.3 on page 136) to set up wireless security.
- Use the **QoS** screen (see Section 7.4 on page 142) to enable or disable wireless quality of service.
- Use the **WPS** screen and the **WPS Station** screen to use WiFi Protected Setup (WPS). WPS lets you set up a secure network quickly, when connecting to other WPS-enabled devices.

  Use the **WPS** screen (see Section 7.5 on page 143) to enable or disable WPS, generate a security PIN (Personal Identification Number) and see information about the ZyXEL Device's WPS status. You can also set up WPS by pressing a button or using a PIN.
- Use the **Scheduling** screen (see Section 7.6 on page 145) to schedule a time period for the wireless LAN to operate each day.
- Use the **Association List** screen (see Section 7.7 on page 147) to view wireless stations that are currently associated with the ZyXEL Device.

You don't necessarily need to use all these screens to set up your wireless connection. For example, you may just want to set up a network name, a wireless radio channel and some security in the **General** and **Security** screens.

7.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter.

Wireless Basics

"Wireless" is essentially radio communication. In the same way that walkie-talkie radios send and receive information over the airwaves, wireless networking devices exchange information with one another. A wireless networking device is just like a radio that lets your computer exchange information with radios attached to other computers. Like walkie-talkies, most wireless networking devices operate at radio frequency bands that are open to the public and do not require a license to use. However, wireless networking is different from that of most traditional radio communications in that there a number of wireless networking standards available with different methods of data encryption.

Wireless Network Construction

Wireless networks consist of wireless clients, access points and bridges.

- A wireless client is a radio connected to a user's computer.
- An access point is a radio with a wired connection to a network, which can connect with numerous wireless clients and let them access the network.
- A bridge is a radio that relays communications between access points and wireless clients, extending a network's range.

Traditionally, a wireless network operates in one of two ways.

- An “infrastructure” type of network has one or more access points and one or more wireless clients. The wireless clients connect to the access points.
- An “ad-hoc” type of network is one in which there is no access point. Wireless clients connect to one another in order to exchange information.

Network Names

Each network must have a name, referred to as the SSID - “Service Set IDentifier”. The “service set” is the network, so the “service set identifier” is the network’s name. This helps you identify your wireless network when wireless networks’ coverage areas overlap and you have a variety of networks to choose from.

Multiple SSIDs

Traditionally, you needed to use different access points (APs) to configure different SSIDs. As well as the cost of buying extra APs, there is also the possibility of channel interference. The ZyXEL Device’s Multiple SSID function allows you to use one AP to provide several SSIDs simultaneously. You can then assign varying levels of privilege to different SSIDs.

Wireless stations can use different SSIDs to associate with the same AP.

The following are some notes on multiple SSIDs.

- A maximum of four SSIDs can be used simultaneously.
- You must use different WEP keys for different BSSs. If two stations have different SSIDs, but have the same WEP keys, they may hear each other’s communications (but not communicate with each other).

Radio Channels

In the radio spectrum, there are certain frequency bands allocated for unlicensed, civilian use. For the purposes of wireless networking, these bands are divided into numerous channels. This allows a variety of networks to exist in the same place without interfering with one another. When you create a network, you must select a channel to use.

Since the available unlicensed spectrum varies from one country to another, the number of available channels also varies.

Wireless Security

By their nature, radio communications are simple to intercept. For wireless data networks, this means that anyone within range of a wireless network without

security can not only read the data passing over the airwaves, but also join the network. Once an unauthorized person has access to the network s/he can either steal information or introduce malware (malicious software) intended to compromise the network. For these reasons, a variety of security systems have been developed to ensure that only authorized people can use a wireless data network, or understand the data carried on it.

These security standards do two things. First, they authenticate. This means that only people presenting the right credentials (often a username and password, or a “key” phrase) can access the network. Second, they encrypt. This means that the information sent over the air is encoded. Only people with the code key can understand the information, and only people who have been authenticated are given the code key.

These security standards vary in effectiveness. Some can be broken, such as the old Wired Equivalent Protocol (WEP). Using WEP is better than using no security at all, but it will not keep a determined attacker out. Other security standards are secure in themselves but can be broken if a user does not use them properly. For example, the WPA-PSK security standard is perfectly secure if you use a long key which is difficult for an attacker’s software to guess - for example, a twenty-letter long string of apparently random numbers and letters - but it is not very secure if you use a short key which is very easy to guess - for example, a three-letter word from the dictionary.

Because of the damage that can be done by a malicious attacker, it’s not just people who have sensitive information on their network who should use security. Everybody who uses any wireless network should ensure that effective security is in place.

A good way to come up with effective security keys, passwords and so on is to use obscure information that you personally will easily remember, and to enter it in a way that appears random and does not include real words. For example, if your mother owns a 1970 Dodge Challenger and her favorite movie is Vanishing Point (which you know was made in 1971) you could use “70dodchal71vanpoi” as your security key.

Signal Problems

Because wireless networks are radio networks, their signals are subject to limitations of distance, interference and absorption.

Problems with distance occur when the two radios are too far apart. Problems with interference occur when other radio waves interrupt the data signal. Interference may come from other radio transmissions, such as military or air traffic control communications, or from machines that are coincidental emitters such as electric motors or microwaves. Problems with absorption occur when physical objects (such as thick walls) are between the two radios, muffling the signal.

7.1.3 Before You Begin

Before you start using these screens, ask yourself the following questions. See Section 7.1.2 on page 130 if some of the terms used here do not make sense to you.

- What wireless standards do the other wireless devices support (IEEE 802.11g, for example)? What is the most appropriate standard to use?
- What security options do the other wireless devices support (WPA-PSK, for example)? What is the best one to use?
- Do the other wireless devices support WPS (Wi-Fi Protected Setup)? If so, you can set up a well-secured network very easily.

  Even if some of your devices support WPS and some do not, you can use WPS to set up your network and then add the non-WPS devices manually, although this is somewhat more complicated to do.
- What advanced options do you want to configure, if any? If you want to configure advanced options, ensure that you know precisely what you want to do. If you do not want to configure advanced options, leave them alone.

7.2 The Wireless LAN General Screen

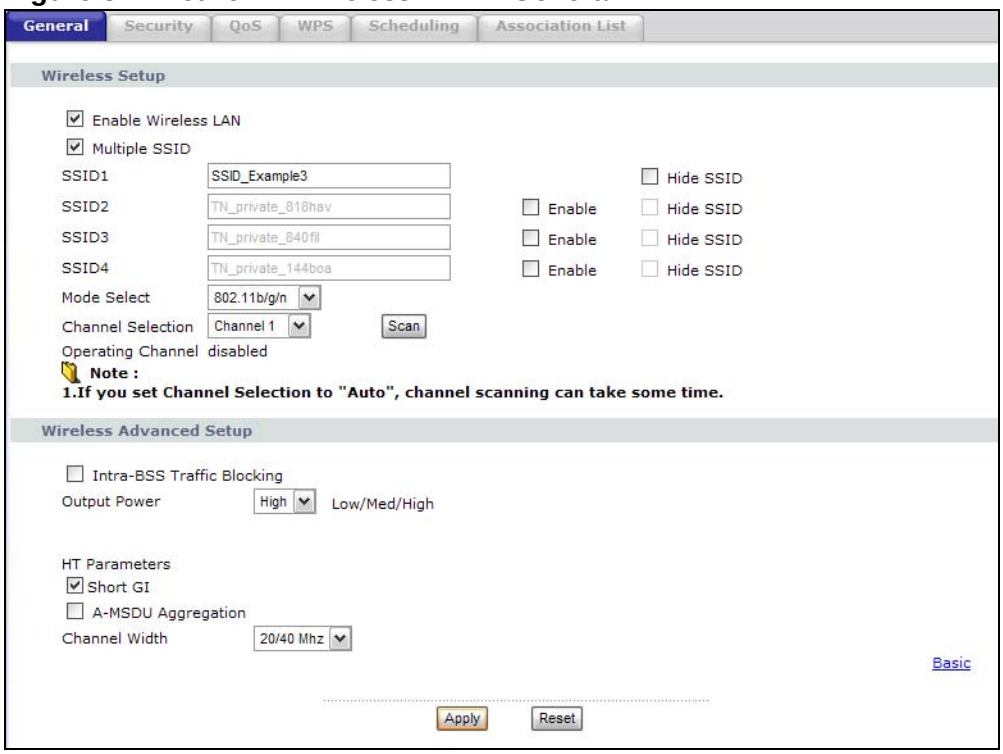
Use this screen to turn the wireless connection on or off, create multiple SSIDs and make other configuration changes.

The ZyXEL Device can broadcast up to four wireless network names at the same time. This means that users can connect to the ZyXEL Device using different SSIDs. You can secure the connection on each SSID profile so that wireless clients connecting to the ZyXEL Device using different SSIDs cannot communicate with each other.

Note: If you are configuring the ZyXEL Device from a computer connected to the wireless LAN and you change the ZyXEL Device's SSID or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the ZyXEL Device's new settings.

Click **Network > Wireless LAN** to open the **General** screen.

Figure 34 Network > Wireless LAN > General



The following table describes the labels in this screen.

Table 24 Network > Wireless LAN > General

LABEL	DESCRIPTION
Enable Wireless LAN	Check this to activate wireless LAN.
Multiple SSID	Check this to have the ZyXEL Device broadcast more than one SSID.
SSID1 ~ SSID 4	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. Enter the SSID you want to use. If you want to use more than one SSID, check **Multiple SSID**, enter the SSID(s) in the field(s) and click **Enable**. You can enable up to four SSIDs simultaneously, and each SSID can have its own security configuration (refer to Section 7.3 on page 136 for setting the wireless security). Note: **SSID1** is enabled by default and cannot be disabled.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.

Table 24 Network > Wireless LAN > General (continued)

LABEL	DESCRIPTION
Mode Select	This makes sure that only compliant WLAN devices can associate with the ZyXEL Device. Select **802.11b/g/n** to allow IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the ZyXEL Device. The transmission rate of your ZyXEL Device might be reduced. Select **802.11b/g** to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the ZyXEL Device. The transmission rate of your ZyXEL Device might be reduced. Select **802.11g** Only to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device. Select **802.11n only in 2.4G band** to allow only IEEE 802.11n compliant WLAN devices with the same frequency range (2.4 GHz) to associate with the ZyXEL Device. Select **802.11n only in 5G band** to allow only IEEE 802.11n compliant WLAN devices with the same frequency range (5 GHz) to associate with the ZyXEL Device.
Channel Selection	Select this option and set the operating frequency/channel depending on your particular region. Select a channel from the drop-down list box.
Scan	Click this button to have the ZyXEL Device immediately scan for and select a channel which is not used by another device.
Operating Channel	The ZyXEL Device automatically scans for and selects a channel whenever the device reboots or the wireless setting is changed. This is the channel currently being used by your AP.
Intra-BSS Traffic Blocking	A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP). Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client A and B can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless client A and B can still access the wired network but cannot communicate with each other. Check this to prevent wireless clients in this wireless network from communicating with one another.
Output Power	Set the output power of the ZyXEL Device in this field. If there is a high density of wireless devices in an area, decrease the output power of the ZyXEL Device to reduce interference with other wireless devices. Select either **Low**, **Med** or **High**. See the product specifications for more information on your ZyXEL Device's output power.
HT Parameters	HT (High Throughput) - Use the fields below to configure the 802.11n wireless environment of your ZyXEL Device.

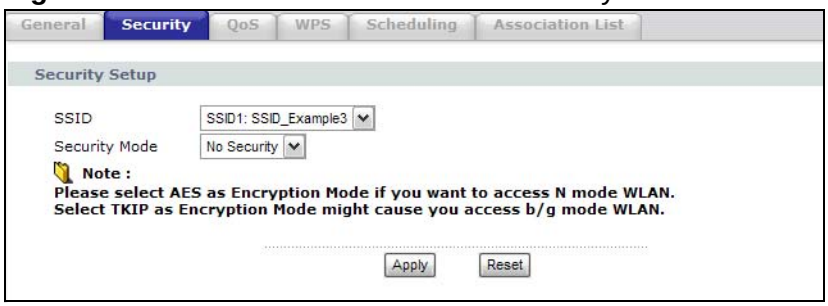
Table 24 Network > Wireless LAN > General (continued)

LABEL	DESCRIPTION
Short GI	This field displays only when you select **802.11b/g/n**, **802.11n only in 2.4G band** or **802.11n only in 5G band** in the **Mode Select** field. Check this to use **Short GI** (Guard Interval). The guard interval is the gap introduced between data transmission from users in order to reduce interference. Reducing the GI increases data transfer rates but also increases interference. Increasing the GI reduces data transfer rates but also reduces interference.
A-MPDU Aggregation	This field displays only when you select **802.11b/g/n**, **802.11n only in 2.4G band** or **802.11n only in 5G band** in the **Mode Select** field. Check this to allow the grouping of several A-MSDUs (Aggregate MAC Service Data Units) into one large A-MPDU (Aggregate MAC Protocol Data Unit). This function allows faster data transfer rates.
Channel Width	This field displays only when you select **802.11b/g/n**, **802.11n only in 2.4G band** or **802.11n only in 5G band** in the **Mode Select** field. A standard 20MHz channel offers transfer speeds of up to 150Mbps whereas a 40MHz channel uses two standard channels and offers speeds of up to 300Mbps. However, not all devices support 40MHz channels. Select the channel bandwidth you want to use for your wireless network. It is recommended that you select **20/40** (20/40 MHz). This allows the ZyXEL Device to adjust the channel bandwidth depending on network conditions. Select **20 MHz** if you want to lessen radio interference with other wireless devices in your neighborhood.
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to reload the previous configuration for this screen.

7.3 The Security Screens

Use this screen to set up wireless security of your ZyXEL Device. Click **Network > Wireless LAN > Security** to open the following screen. The screen varies depending on the wireless security you select.

Figure 35 Network > Wireless LAN > Security



The following table describes the labels in this screen.

Table 25 Network > Wireless LAN > Security

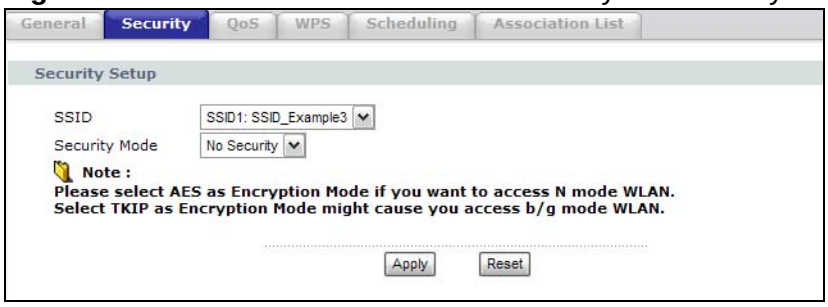
LABEL	DESCRIPTION
SSID	Select the SSID security profile you want to configure.
Security Mode	Select **Static WEP**, **Shared WEP**, **WPA-PSK**, **WPA2-PSK**, **WPA** or **WPA2** to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as this device. After you select to use a security, additional options appears in this screen. See 7.3.2, 7.3.3, 7.3.4 sections. Or you can select **No Security** to allow any client to associate this network without authentication. Note: If you enable the WPS function, only **No Security**, **WPA-PSK** and **WPA2-PSK** are available in this option.
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to reload the previous configuration for this screen.

7.3.1 No Security

Select **No Security** to allow wireless devices to communicate with the access points without any data encryption.

Note: If you do not enable any wireless security on your ZyXEL Device, your network is accessible to any wireless networking device that is within range.

Figure 36 Network > Wireless LAN > Security: No Security



7.3.2 Static WEP/Shared WEP Encryption

WEP encryption scrambles the data transmitted between the wireless stations and the access points (AP) to keep network communications private. Both the wireless stations and the access points must use the same WEP key.

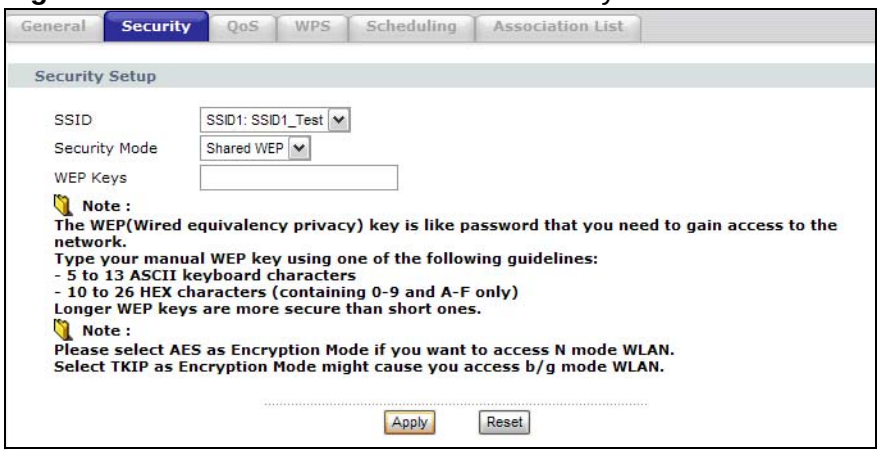
There are two types of WEP authentication namely, Open System (**Static WEP**) and Shared Key (**Shared WEP**).

Open system is implemented for ease-of-use and when security is not an issue. The wireless station and the AP or peer computer do not share a secret key. Thus

the wireless stations can associate with any AP or peer computer and listen to any transmitted data that is not encrypted.

Shared key mode involves a shared secret key to authenticate the wireless station to the AP or peer computer. This requires you to enable the wireless LAN security and use same settings on both the wireless station and the AP or peer computer. In order to configure and enable WEP encryption, click **Network > Wireless LAN > Security**. Select **Static WEP** or **Shared WEP** from the **Security Mode** list.

Figure 37 Network > Wireless LAN > Security: Static WEP/Shared WEP


General
Security
QoS
WPS
Scheduling
Association List
Security Setup
SSID
SSID1: SSID1_Test
Security Mode
Shared WEP
WEP Keys
Note :
The WEP(Wired equivalency privacy) key is like password that you need to gain access to the network.
Type your manual WEP key using one of the following guidelines:
- 5 to 13 ASCII keyboard characters
- 10 to 26 HEX characters (containing 0-9 and A-F only)
Longer WEP keys are more secure than short ones.
Note :
Please select AES as Encryption Mode if you want to access N mode WLAN.
Select TKIP as Encryption Mode might cause you access b/g mode WLAN.
Apply
Reset

The following table describes the wireless LAN security labels in this screen.

Table 26 Network > Wireless LAN > Security: Static WEP/Shared WEP

LABEL	DESCRIPTION
SSID	Select the SSID security profile you want to configure.
Security Mode	Choose **Static WEP or Shared WEP** from the drop-down list box. • Select **Static WEP** to have the ZyXEL Device allow association with wireless clients that use Open System mode. Data transfer is encrypted as long as the wireless client has the correct WEP key for encryption. The ZyXEL Device authenticates wireless clients using Shared Key mode that have the correct WEP key. • Select **Shared WEP** to have the ZyXEL Device authenticate only those wireless clients that use Shared Key mode and have the correct WEP key.
WEP Keys	Enter a WEP key that will be used to encrypt data. Both the ZyXEL Device and the wireless stations must use the same WEP key for data transmission. If you want to manually set the WEP key, enter any 5 or 13 characters (ASCII string) or 10 or 26 hexadecimal characters ("0-9", "A-F") for a 64-bit or 128-bit WEP key respectively.
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to reload the previous configuration for this screen.

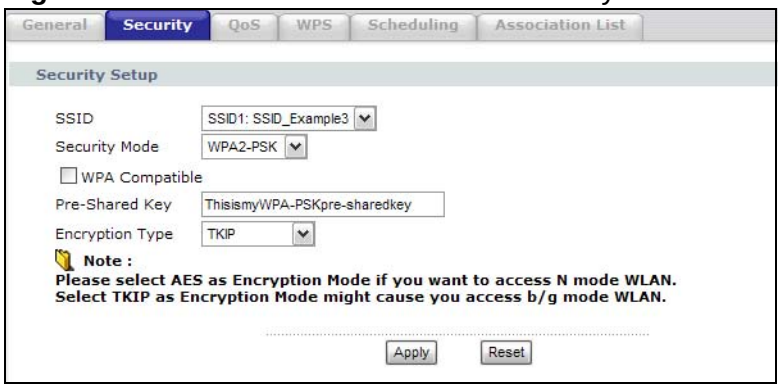
7.3.3 WPA-PSK/WPA2-PSK Authentication

The WPA-PSK security mode provides both improved data encryption and user authentication over WEP. Using a Pre-Shared Key (PSK), both the ZyXEL Device and the connecting client share a common password in order to validate the connection. This type of encryption, while robust, is not as strong as WPA, WPA2 or even WPA2-PSK. The WPA2-PSK security mode is a newer, more robust version of the WPA encryption standard. It offers slightly better security, although the use of PSK makes it less robust than it could be.

Use these options if you do not have RADIUS server on your network to verify user credentials.

Click **Network > Wireless LAN > Security** and select **WPA-PSK** or **WPA2-PSK** from the **Security Mode** list.

Figure 38 Network > Wireless LAN > Security: WPA-PSK/WPA2-PSK



The following table describes the wireless LAN security labels in this screen.

Table 27 Network > Wireless LAN > Security: WPA-PSK/WPA2-PSK

LABEL	DESCRIPTION
SSID	Select the SSID security profile you want to configure.
Security Mode	Choose **WPA-PSK** or **WPA2-PSK** from the drop-down list box.
WPA Compatible	This field is only available for WPA2-PSK. Select this if you want the ZyXEL Device to support WPA-PSK and WPA2-PSK simultaneously.
Pre-Shared Key	The encryption mechanisms used for **WPA / WPA2** and **WPA-PSK / WPA2-PSK** are the same. The only difference between the two is that **WPA-PSK / WPA2-PSK** uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).

Table 27 Network > Wireless LAN > Security: WPA-PSK/WPA2-PSK

LABEL	DESCRIPTION
Encryption Type	Select **TKIP** to enable Temporal Key Integrity Protocol (TKIP) security on your wireless network. Use this if the other access points on your network support do not have an AES option. Select **AES** to enable Advanced Encryption System (AES) security on your wireless network. AES provides superior security to TKIP. Use AES if the other access points on your network support it. Select **TKIPAES MIX** to allow both TKIP and AES types of security in your wireless network.
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to reload the previous configuration for this screen.

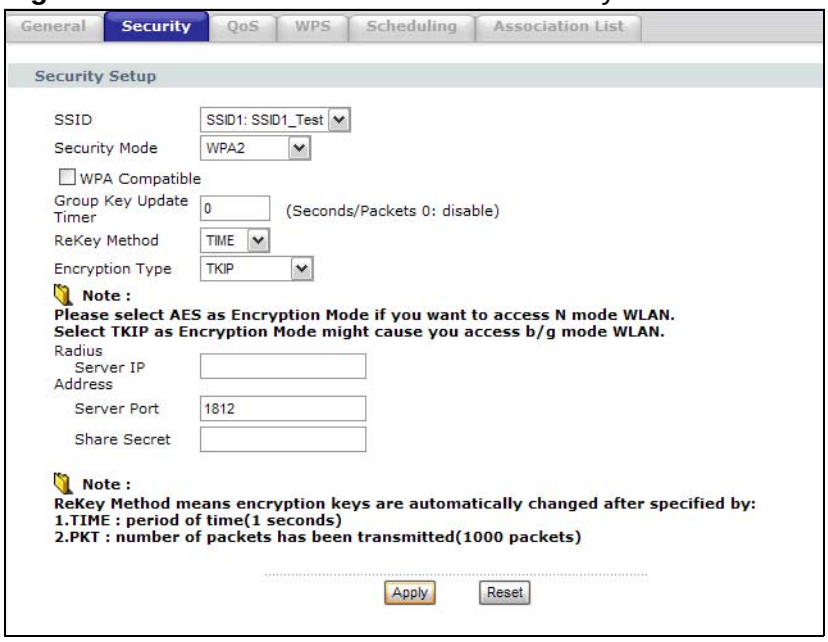
7.3.4 WPA/WPA2 Authentication

The WPA2 security mode is currently the most robust form of encryption for wireless networks. It requires a RADIUS server to authenticate user credentials and is a full implementation the security protocol. Use this security option for maximum protection of your network. However, it is the least backwards compatible with older devices.

The WPA security mode is a security subset of WPA2. It requires the presence of a RADIUS server on your network in order to validate user credentials. This encryption standard is slightly older than WPA2 and therefore is more compatible with older devices.

Click **Network > Wireless LAN > Security** and select **WPA** or **WPA2** from the **Security Mode** list.

Figure 39 Network > Wireless LAN > Security: WPA/WPA2



The following table describes the wireless LAN security labels in this screen.

Table 28 Network > Wireless LAN > Security: WPA/WPA2

LABEL	DESCRIPTION
SSID	Select the SSID security profile you want to configure.
Security Mode	Choose **WPA** or **WPA2** from the drop-down list box.
WPA Compatible	This field is only available for WPA2. Select this if you want the ZyXEL Device to support WPA and WPA2 simultaneously.
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP (if using **WPA(2)-PSK** key management) or **RADIUS** server (if using WPA(2) key management) sends a new group key out to all clients. Setting of the **Group Key Update Timer** is also supported in **WPA(2)-PSK** mode. The ZyXEL Device default is **1800** seconds (30 minutes).
ReKey Method	• The ZyXEL Device can automatically disconnect a wireless station from the wired network after a period of inactivity or after a certain number of packets have been processed. The wireless station needs to enter the username and password again before access to the wired network is allowed. Select **TIME** to have the ZyXEL Device automatically disconnects a wireless station from the wired network after a period of inactivity. • Select **PKT** to have the ZyXEL Device automatically disconnects a wireless station from the wired network after a certain number of packets have been processed. • Select **NONE** if you do not want the connection between the ZyXEL Device and a wireless station to time out.

Table 28 Network > Wireless LAN > Security: WPA/WPA2

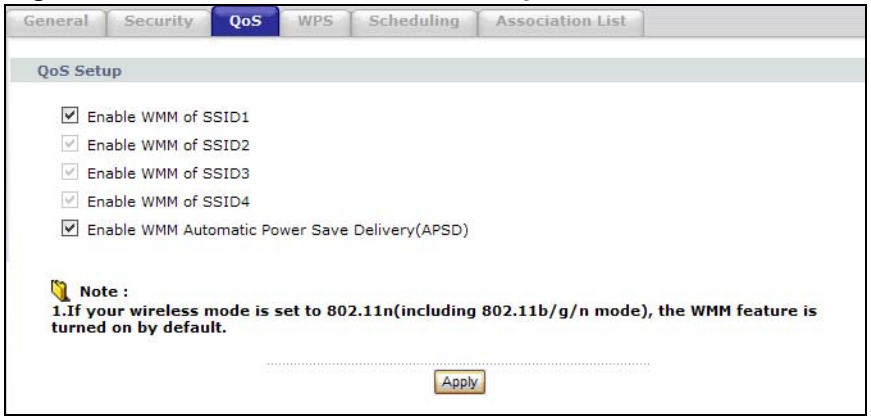
LABEL	DESCRIPTION
Encryption Type	Select **TKIP** to enable Temporal Key Integrity Protocol (TKIP) security on your wireless network. Use this if the other access points on your network support do not have an AES option. Select **AES** to enable Advanced Encryption System (AES) security on your wireless network. AES provides superior security to TKIP. Use AES if the other access points on your network support it. Select **TKIPAES MIX** to allow both TKIP and AES types of security in your wireless network.
Radius	
Server IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Server Port	Enter the port number of the external authentication server. The default port number is **1812**. You need not change this value unless your network administrator instructs you to do so with additional information.
Share Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the ZyXEL Device. The key must be the same on the external authentication server and your ZyXEL Device. The key is not sent over the network.
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to reload the previous configuration for this screen.

7.4 The QoS Screen

This screen allows you to enable or disable wireless quality of service.

Click **Network > Wireless LAN** > **QoS**. The following screen displays.

Figure 40 Network > Wireless LAN > QoS



The following table describes the labels in this screen.

Table 29 Network > Wireless LAN > QoS

LABEL	DESCRIPTION
Enable WMM of SSID1~4	Check this to have the ZyXEL Device automatically give a service a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (Wifi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly.
Enable WMM Automatic Power Save Deliver (APSD)	Click this to increase battery life for battery-powered wireless clients. APSD uses a longer beacon interval when transmitting traffic that does not require a short packet exchange interval.
Apply	Click this to save your changes back to the ZyXEL Device.

7.5 WPS

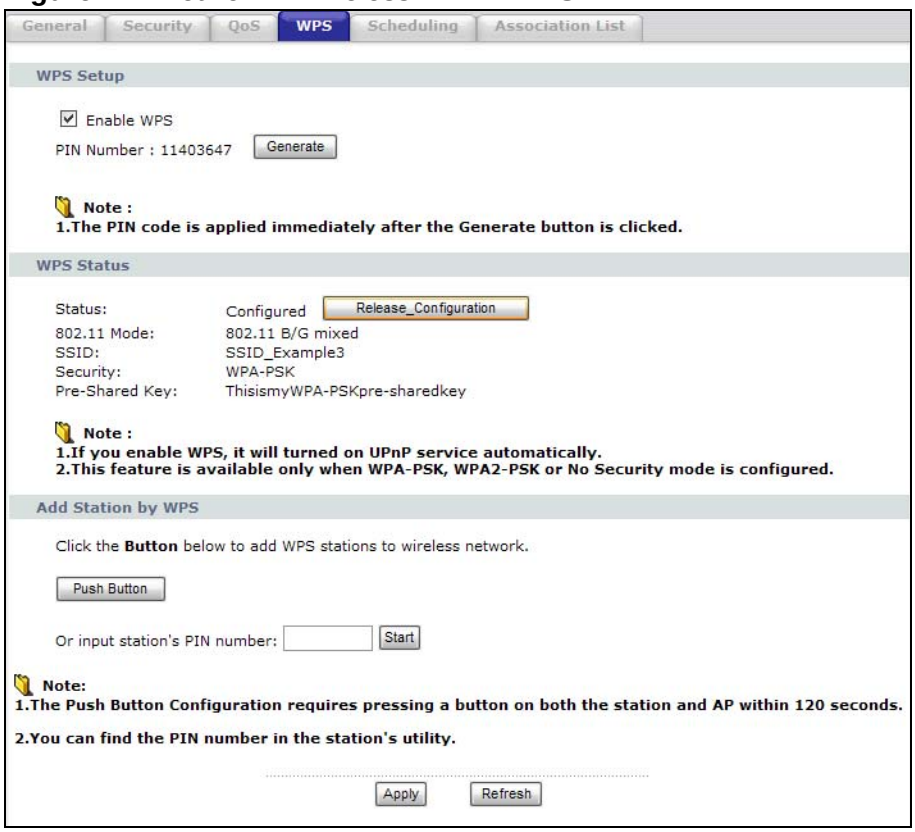
Use this screen to configure WiFi Protected Setup (WPS) on your ZyXEL Device.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Set up each WPS connection between two devices. Both devices must support WPS. See Appendix D on page 345 for more information about WPS.

Note: The ZyXEL Device applies the security settings of the **SSID1** profile (see Section 7.2 on page 133). If you want to use the WPS feature, make sure you have set the security mode of **SSID1** to **WPA-PSK**, **WPA2-PSK** or **No Security**.

Click **Network > Wireless LAN >WPS**. The following screen displays.

Figure 41 Network > Wireless LAN > WPS



The following table describes the labels in this screen.

Table 30 Network > Wireless LAN > WPS

LABEL	DESCRIPTION
Enable WPS	Select the check box to activate WPS on the ZyXEL Device.
PIN Number	This shows the PIN (Personal Identification Number) of the ZyXEL Device. Enter this PIN in the configuration utility of the device you want to connect to using WPS. The PIN is not necessary when you use WPS push-button method.
Generate	Click this button to have the ZyXEL Device create a new PIN.
WPS Status	This displays **Configured** when the ZyXEL Device has connected to a wireless network using WPS or **Enable WPS** is selected and wireless or wireless security settings have been changed. The current wireless and wireless security settings also appear in the screen. This displays **Unconfigured** if WPS is disabled and there is no wireless or wireless security changes on the ZyXEL Device or you click **Release_Configuration** to remove the configured wireless and wireless security settings.
Release Configuration	This button is available when the WPS status is **Configured.** Click this button to remove all configured wireless and wireless security settings for WPS connections on the ZyXEL Device.

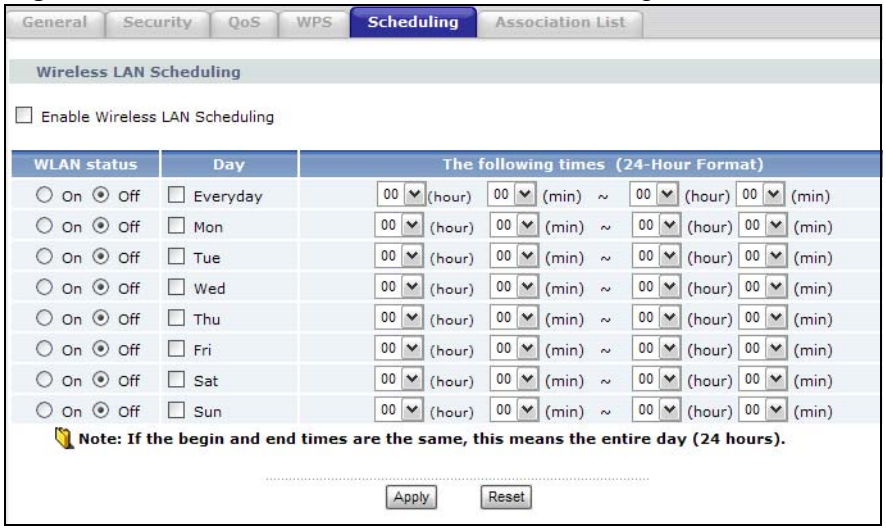
Table 30 Network > Wireless LAN > WPS

LABEL	DESCRIPTION
Add Station by WPS	Use this section to set up a WPS wireless network using either Push Button Configuration (PBC) or PIN Configuration.
Push Button	Click this button to add another WPS-enabled wireless device (within wireless range of the ZyXEL Device) to your wireless network. This button may either be a physical button on the outside of device, or a menu button similar to the **Push Button** on this screen. Note: You must press the other wireless device's WPS button within two minutes of pressing this button.
Or input station's PIN number	Enter the PIN of the device that you are setting up a WPS connection with and click **Start** to authenticate and add the wireless device to your wireless network. You can find the PIN either on the outside of the device, or by checking the device's settings. Note: You must also activate WPS on that device within two minutes to have it present its PIN to the ZyXEL Device.
Apply	Click this to save your changes back to the ZyXEL Device.
Refresh	Click this to reload the previous configuration for this screen.

7.6 Scheduling Screen

Click **Network > Wireless LAN > Scheduling** to open the **Wireless LAN Scheduling** screen. Use this screen to configure when the ZyXEL Device enables or disables the wireless LAN.

Figure 42 Network > Wireless LAN > Scheduling



The following table describes the labels in this screen.

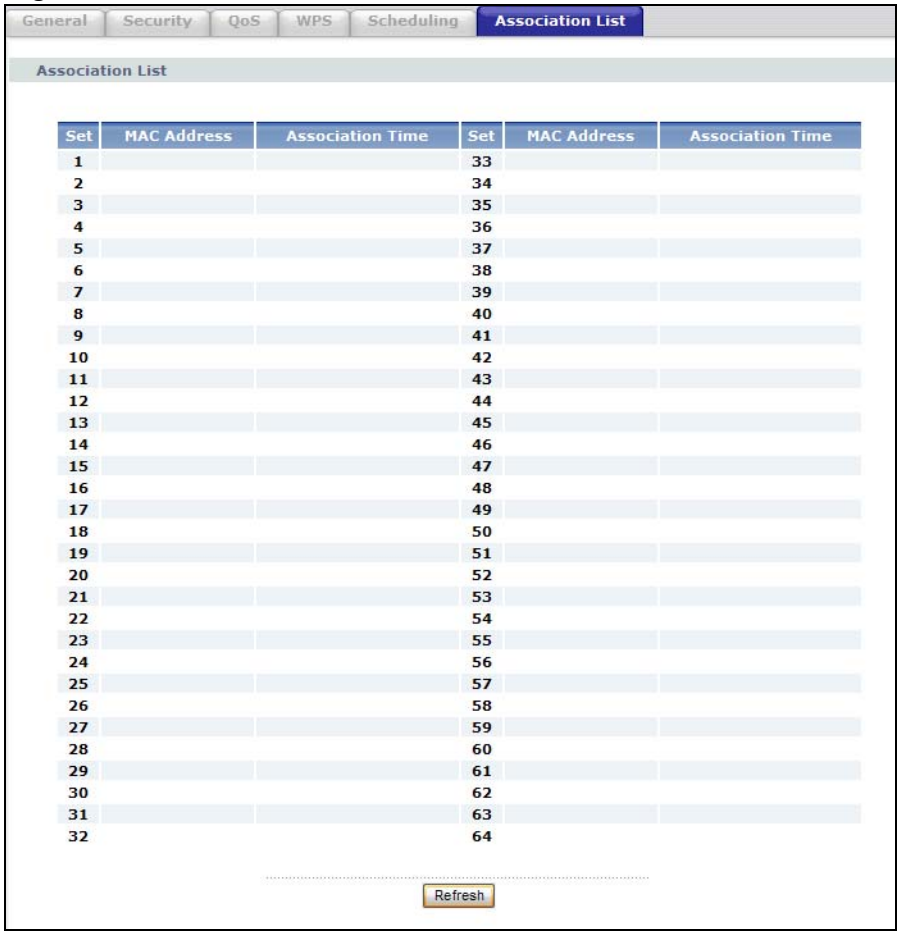
Table 31 Network > Wireless LAN > Scheduling

LABEL	DESCRIPTION
Enable Wireless LAN Scheduling	Select this to activate wireless LAN scheduling on your ZyXEL Device.
WLAN status	Select **On** or **Off** to enable or disable the wireless LAN.
Day	Select the day(s) you want to turn the wireless LAN on or off.
The following times	Specify the time period during which to apply the schedule. For example, you want the wireless network to be only available during work hours. Check Mon ~ Fri in the day column, and specify 8:00 ~ 18:00 in the time table.
Apply	Click this to save your changes.
Reset	Click this to restore your previously saved settings.

7.7 Association List Screen

Use this screen to view wireless stations that are currently associated with the ZyXEL Device. Click **Network > Wireless LAN > Association List** to open the following screen. The screen varies depending on the wireless security you select.

Figure 43 Network > Wireless LAN > Association List



The following table describes the labels in this screen.

Table 32 Association List

LABEL	DESCRIPTION
Set	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC address of an associated wireless station.
Association Time	This field displays the time a wireless station first associated with the ZyXEL Device.
Refresh	Click this to reload the screen.

7.8 Wireless LAN Technical Reference

The following section contains additional technical information about the ZyXEL Device features described in this chapter.

The following table describes some wireless network terms and acronyms used in the ZyXEL Device's Web Configurator.

Table 33 Additional Wireless Terms

TERM	DESCRIPTION
RTS/CTS Threshold	In a wireless network which covers a large area, wireless devices are sometimes not aware of each other's presence. This may cause them to send information to the AP at the same time and result in information colliding and not getting through. By setting this value lower than the default value, the wireless devices must sometimes get permission to send information to the ZyXEL Device. The lower the value, the more often the devices must get permission. If this value is greater than the fragmentation threshold value (see below), then wireless devices never have to get permission to send information to the ZyXEL Device.
Authentication	The process of verifying whether a wireless device is allowed to use the wireless network.
Fragmentation Threshold	A small fragmentation threshold is recommended for busy networks, while a larger threshold provides faster performance if the network is not very busy.

Refer to Appendix D on page 345 for more information.

8

Network Address Translation (NAT)

8.1 Overview

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

8.1.1 What You Can Do in this Chapter

Use the **Port Forwarding** screen (Section 8.2 on page 150) to configure forward incoming service requests to the server(s) on your local network.

8.1.2 What You Need To Know

The following terms and concepts may help as you read this chapter.

Inside/Outside and Global/Local

Inside/outside denotes where a host is located relative to the ZyXEL Device, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

NAT

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back,

NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host.

Port Forwarding

A port forwarding set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single computer to the outside world.

Finding Out More

See Section 8.3 on page 154 for advanced technical information on NAT.

8.2 Port Forwarding

Use the **Port Forwarding** screen to forward incoming service requests to the server(s) on your local network.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

The most often used port numbers and services are shown in Appendix E on page 369. Please refer to RFC 1700 for further information about port numbers.

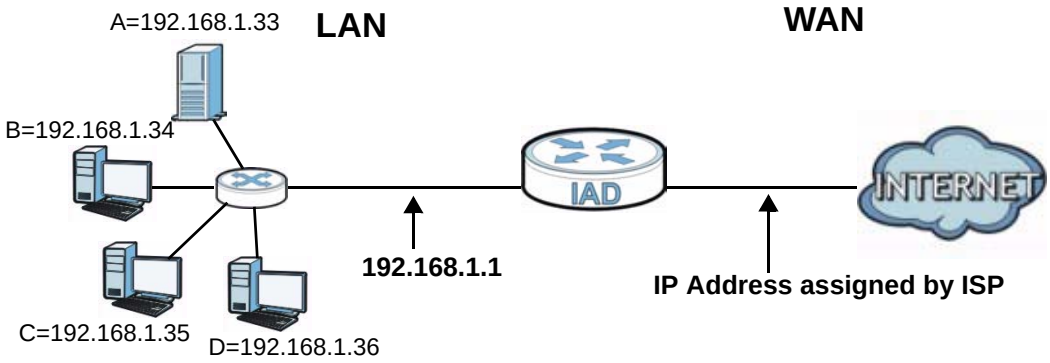
Note: Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

Configuring Servers Behind Port Forwarding (Example)

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP

addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 44 Multiple Servers Behind NAT Example

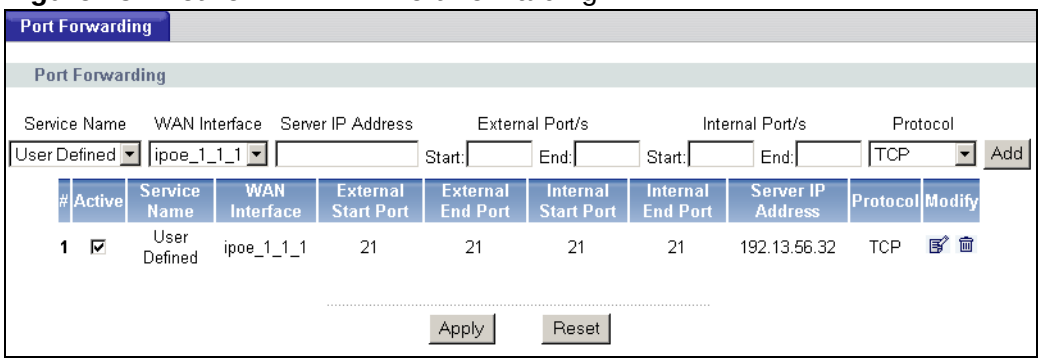


8.2.1 Configuring the Port Forwarding Screen

Click **Network > NAT > Port Forwarding** to open the following screen.

See Appendix E on page 369 for port numbers commonly used for particular services.

Figure 45 Network > NAT > Port Forwarding



The following table describes the fields in this screen.

Table 34 Network > NAT > Port Forwarding

LABEL	DESCRIPTION
Port Forwarding	
Service Name	Select a pre-defined service from the drop-down list box. The pre-defined service port number(s) and protocol will display in the **External port**, **Internal port** and **Protocol** fields. Otherwise, select **User Defined** and manually enter the port number(s) and select the IP protocol.
WAN Interface	Select the WAN interface through which the service is forwarded. You must have already configured a WAN connection with NAT enabled.

Table 34 Network > NAT > Port Forwarding

LABEL	DESCRIPTION
Server IP Address	Enter the IP address of the server for the specified service.
External Port Start	Enter the original destination port for the packets. To forward only one port, enter the port number again in the **External Port End** field. To forward a series of ports, enter the start port number here and the end port number in the **External Port End** field.
External Port End	Enter the last port of the original destination port range. To forward only one port, enter the port number in the **External Port Start** field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the **External Port Start** field above.
Internal Port Start	This shows the port number to which you want the ZyXEL Device to translate the incoming port.
Internal Port End	This shows the last port of the translated port range.
Protocol	Select the protocol supported by this virtual server. Choices are **TCP**, **UDP**, or **TCP/UDP**.
Add	Click this button to add a rule to the table below.
The table below shows a summary of the values entered in the previous fields.	
#	This is the rule index number (read-only).
Active	This field indicates whether the rule is active or not. Clear the check box to disable the rule. Select the check box to enable it.
Service Name	This is the service's name. This shows **User Defined** if you manually added a service. You can change this by clicking the edit icon.
WAN Interface	This shows the WAN interface through which the service is forwarded.
External Start Port	This is the first external port number that identifies a service.
External End Port	This is the last external port number that identifies a service.
Internal Start Port	This is the first internal port number that identifies a service.
Internal End Port	This is the last internal port number that identifies a service.
Server IP Address	This is the server's IP address.
Protocol	This shows the IP protocol supported by this virtual server, whether it is **TCP**, **UDP**, or **TCP/UDP**.

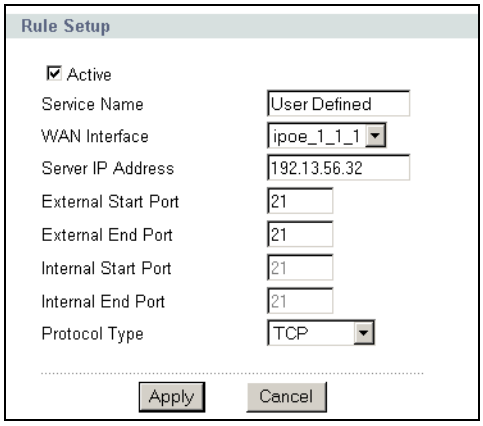
Table 34 Network > NAT > Port Forwarding

LABEL	DESCRIPTION
Modify	Click the edit icon to go to the screen where you can edit the port forwarding rule. Click the delete icon to delete an existing port forwarding rule. Note that subsequent address mapping rules move up by one when you take this action.
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to return to the previous configuration.

8.2.2 The Port Forwarding Edit Screen

This screen lets you create or edit a port forwarding rule. Click the rule's **Edit** icon in the **Port Forwarding** screen to open the following screen.

Figure 46 Port Forwarding Edit



The following table describes the labels in this screen.

Table 35 Port Forwarding Edit

LABEL	DESCRIPTION
Active	Clear the check box to disable the rule. Select the check box to enable it.
Service Name	Enter a name to identify this rule using keyboard characters (A-Z, a-z, 1-2 and so on).
WAN Interface	Select the WAN interface through which the service is forwarded. You must have already configured a WAN connection with NAT enabled.
Server IP Address	Enter the inside IP address of the virtual server here.
External Start Port	Enter the original destination port for the packets. To forward only one port, enter the port number again in the **External End Port** field. To forward a series of ports, enter the start port number here and the end port number in the **External End Port** field.

Table 35 Port Forwarding Edit (continued)

LABEL	DESCRIPTION
External End Port	Enter the last port of the original destination port range. To forward only one port, enter the port number in the **External Start Port** field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the **External Start Port** field above.
Internal Start Port	This shows the port number to which you want the ZyXEL Device to translate the incoming port. For a range of ports, enter the first number of the range to which you want the incoming ports translated.
Internal End Port	This shows the last port of the translated port range.
Protocol Type	Select the protocol supported by this virtual server. Choices are **TCP**, **UDP**, or **TCP / UDP**.
Apply	Click this to save your changes back to the ZyXEL Device.
Cancel	Click this to begin configuring this screen afresh.

8.3 NAT Technical Reference

This section provides some technical background information about the topics covered in this chapter.

8.3.1 NAT Definitions

Inside/outside denotes where a host is located relative to the ZyXEL Device, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside

host when the packet is on the WAN side. The following table summarizes this information.

Table 36 NAT Definitions

ITEM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

NAT never changes the IP address (either local or global) of an outside host.

8.3.2 What NAT Does

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

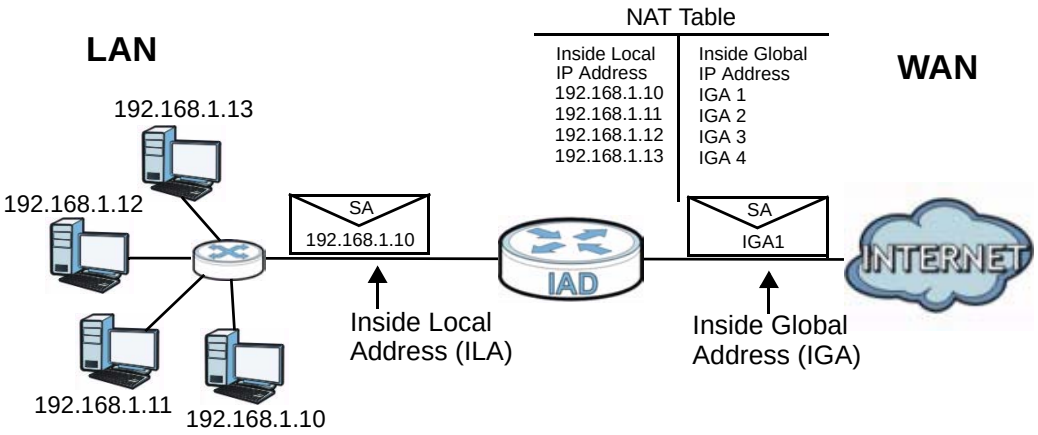
The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers, NAT offers the additional benefit of firewall protection. With no servers defined, your ZyXEL Device filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631*, *The IP Network Address Translator (NAT)*.

8.3.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The ZyXEL Device keeps track of the original addresses

and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

Figure 47 How NAT Works



9 Voice

9.1 Overview

Use this chapter to:

- Connect an analog phone to the ZyXEL Device.
- Make phone calls over the Internet, as well as the regular phone network.
- Configure settings such as speed dial.
- Configure network settings to optimize the voice quality of your phone calls.

9.1.1 What You Can Do in this Chapter

These screens allow you to configure your ZyXEL Device to make phone calls over the Internet and your regular phone line, and to set up the phones you connect to the ZyXEL Device.

- Use the **SIP Service Provider** screen (Section 9.3 on page 165) to configure the SIP server information, QoS for VoIP calls, the numbers for certain phone functions and dialing plan.
- Use the **SIP Account** screen (Section 9.3 on page 165) to set up information about your SIP account, control which SIP accounts the phones connected to the ZyXEL Device use and configure audio settings such as volume levels for the phones connected to the ZyXEL Device.
- Use the **Analog Phone** screen (Section 9.4 on page 169) to control which SIP accounts the phones connected to the ZyXEL Device use.
- Use the **Region** screen (Section 9.5 on page 170) to change settings that depend on the country you are in.
- Use the **Speed Dial** screen (Section 9.6 on page 170) to set up shortcuts for dialing frequently-used (VoIP) phone numbers.

You don't necessarily need to use all these screens to set up your account. In fact, if your service provider did not supply information on a particular field in a screen, it is usually best to leave it at its default setting.

9.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter.

VoIP

VoIP stands for Voice over IP. IP is the Internet Protocol, which is the message-carrying standard the Internet runs on. So, Voice over IP is the sending of voice signals (speech) over the Internet (or another network that uses the Internet Protocol).

SIP

SIP stands for Session Initiation Protocol. SIP is a signalling standard that lets one network device (like a computer or the ZyXEL Device) send messages to another. In VoIP, these messages are about phone calls over the network. For example, when you dial a number on your ZyXEL Device, it sends a SIP message over the network asking the other device (the number you dialed) to take part in the call.

SIP Accounts

A SIP account is a type of VoIP account. It is an arrangement with a service provider that lets you make phone calls over the Internet. When you set the ZyXEL Device to use your SIP account to make calls, the ZyXEL Device is able to send all the information about the phone call to your service provider on the Internet.

Strictly speaking, you don't need a SIP account. It is possible for one SIP device (like the ZyXEL Device) to call another without involving a SIP service provider. However, the networking difficulties involved in doing this make it tremendously impractical under normal circumstances. Your SIP account provider removes these difficulties by taking care of the call routing and setup - figuring out how to get your call to the right place in a way that you and the other person can talk to one another.

How to Find Out More

See Chapter 3 on page 33 for a tutorial showing how to set up these screens in an example scenario.

See Section 9.7 on page 172 for advanced technical information on SIP.

9.1.3 Before You Begin

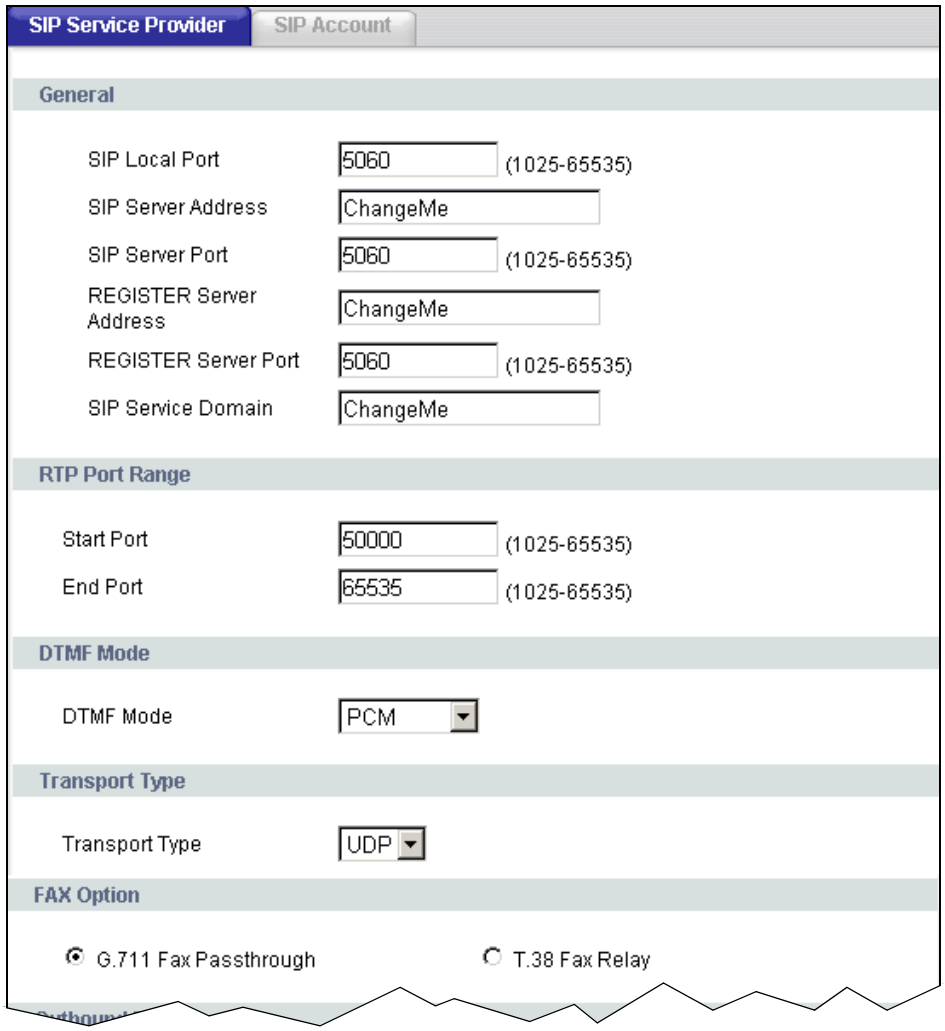
- Before you can use these screens, you need to have a VoIP account already set up. If you don't have one yet, you can sign up with a VoIP service provider over the Internet.
- You should have the information your VoIP service provider gave you ready, before you start to configure the ZyXEL Device.

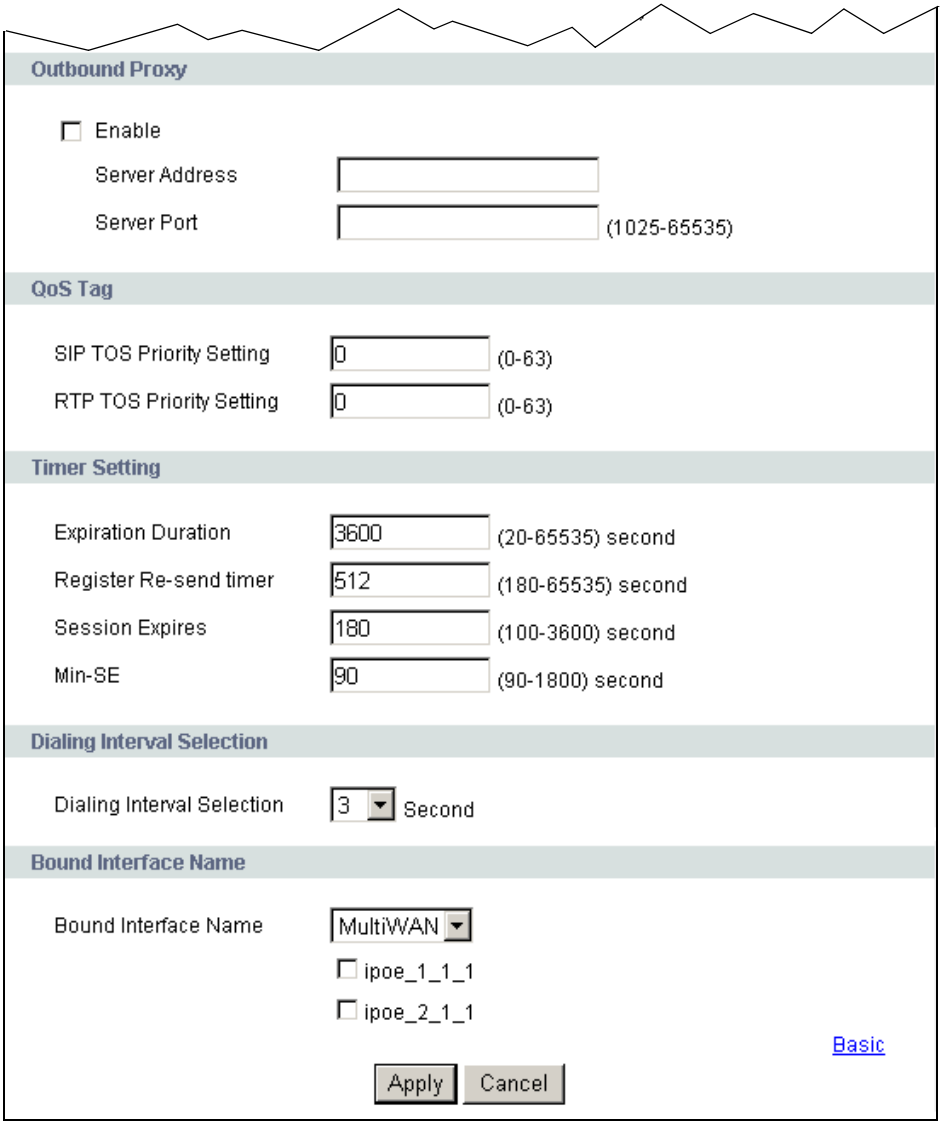
9.2 The SIP Service Provider Screen

Use this screen to configure the SIP server information, QoS for VoIP calls, the numbers for certain phone functions and dialing plan. Click **VoIP > SIP > SIP Service Provider** to open the **SIP Service Provider** screen.

Note: Click **Advanced** to see all the fields in the screen. You don't necessarily need to use all these fields to set up your account. Click **Basic** to see and configure only the fields needed for this feature.

Figure 48 VoIP > SIP > SIP Service Provider (Advanced)





Each field is described in the following table.

Table 37 VoIP > SIP > SIP Service Provider (Advanced)

LABEL	DESCRIPTION
General	
SIP Local Port	Enter the ZyXEL Device's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
SIP Server Address	Enter the IP address or domain name of the SIP server provided by your VoIP service provider. You can use up to 95 printable ASCII characters. It does not matter whether the SIP server is a proxy, redirect or register server.
SIP Server Port	Enter the SIP server's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.

Table 37 VoIP > SIP > SIP Service Provider (Advanced)

LABEL	DESCRIPTION
REGISTER Server Address	Enter the IP address or domain name of the SIP register server, if your VoIP service provider gave you one. Otherwise, enter the same address you entered in the **SIP Server Address** field. You can use up to 95 printable ASCII characters.
REGISTER Server Port	Enter the SIP register server's listening port number, if your VoIP service provider gave you one. Otherwise, enter the same port number you entered in the **SIP Server Port** field.
SIP Service Domain	Enter the SIP service domain name. In the full SIP URI, this is the part after the @ symbol. You can use up to 127 printable ASCII Extended set characters.
RTP Port Range	
Start Port End Port	Enter the listening port number(s) for RTP traffic, if your VoIP service provider gave you this information. Otherwise, keep the default values. To enter one port number, enter the port number in the **Start Port** and **End Port** fields. To enter a range of ports, • enter the port number at the beginning of the range in the **Start Port** field. • enter the port number at the end of the range in the **End Port** field.
DTMF Mode	Control how the ZyXEL Device handles the tones that your telephone makes when you push its buttons. You should use the same mode your VoIP service provider uses. **RFC2833** - send the DTMF tones in RTP packets. **PCM** - send the DTMF tones in the voice data stream. This method works best when you are using a codec that does not use compression (like G.711). Codecs that use compression (like G.729 and G.726) can distort the tones. **SIPInfo** - send the DTMF tones in SIP messages.
Transport Type	
Transport Type	Select the transport layer protocol (**TCP**, **UDP** or **TLS**) used for SIP.
FAX Option	This field controls how the ZyXEL Device handles fax messages.
G.711 Fax Passthrough	Select this if the ZyXEL Device should use G.711 to send fax messages. The peer devices must also use G.711.
T.38 Fax Relay	Select this if the ZyXEL Device should send fax messages as UDP or TCP/IP packets through IP networks. This provides better quality, but it may have inter-operability problems. The peer devices must also use T.38.
Outbound Proxy	
Enable	Select this if your VoIP service provider has a SIP outbound server to handle voice calls. This allows the ZyXEL Device to work with any type of NAT router and eliminates the need for STUN or a SIP ALG. Turn off any SIP ALG on a NAT router in front of the ZyXEL Device to keep it from re-translating the IP address (since this is already handled by the outbound proxy server).
Server Address	Enter the IP address or domain name of the SIP outbound proxy server.

Table 37 VoIP > SIP > SIP Service Provider (Advanced)

LABEL	DESCRIPTION
Server Port	Enter the SIP outbound proxy server's listening port, if your VoIP service provider gave you one. Otherwise, keep the default value.
QoS Tag	
SIP TOS Priority Setting	Enter the DSCP (DiffServ Code Point) number for SIP voice transmissions. The ZyXEL Device creates Class of Service (CoS) priority tags with this number to voice traffic that it transmits.
RTP TOS Priority Setting	Enter the DSCP (DiffServ Code Point) number for RTP voice transmissions. The ZyXEL Device creates Class of Service (CoS) priority tags with this number to RTP traffic that it transmits.
Timer Setting	
Expiration Duration	Enter the number of seconds your SIP account is registered with the SIP register server before it is deleted. The ZyXEL Device automatically tries to re-register your SIP account when one-half of this time has passed. (The SIP register server might have a different expiration.)
Register Re-send timer	Enter the number of seconds the ZyXEL Device waits before it tries again to register the SIP account, if the first try failed or if there is no response.
Session Expires	Enter the number of seconds the ZyXEL Device lets a SIP session remain idle (without traffic) before it automatically disconnects the session.
Min-SE	Enter the minimum number of seconds the ZyXEL Device lets a SIP session remain idle (without traffic) before it automatically disconnects the session. When two SIP devices start a SIP session, they must agree on an expiration time for idle sessions. This field is the shortest expiration time that the ZyXEL Device accepts.
Dialing Interval Selection	
Dialing Interval Selection	Enter the number of seconds the ZyXEL Device should wait after you stop dialing numbers before it makes the phone call. The value depends on how quickly you dial phone numbers. If you select **Immediate Dial Enable**, you can press the pound key (#) to tell the ZyXEL Device to make the phone call immediately, regardless of this setting.
Bound Interface Name	
Bound Interface Name	If you select **LAN** or **AnyWAN**, the ZyXEL Device automatically activates the VoIP service when any LAN or WAN connection is up. If you select **MultiWAN**, you also need to select the pre-configured WAN connections. The VoIP service is activated only when the selected WAN connection in ATM mode is up.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.

9.2.1 Dial Plan Rules

A dial plan defines the dialing patterns, such as the length and range of the digits for a telephone number. It also includes country codes, access codes, area codes,

local numbers, long distance numbers or international call prefixes. For example, the dial plan ([2-9]xxxxxx) does not allow a local number which begins with 1 or 0.

Without a dial plan, users have to manually enter the whole callee's number and wait for the specified dialing interval to time out or press a terminator key (usually the pound key on the phone keypad) before the ZyXEL Device makes the call.

The ZyXEL Device initializes a call when the dialed number matches any one of the rules in the dial plan. Dial plan rules follow these conventions:

- The collection of rules is in parentheses ().
- Rules are separated by the | (bar) symbol.
- "x" stands for a wildcard and can be any digit from 0 to 9.
- A subset of keys is in a square bracket []. Ranges are allowed.

  For example, [359] means a number matching this rule can be 3, 5 or 9. [26-8*] means a number matching this rule can be 2, 6, 7, 8 or *.
- The dot "." appended to a digit allows the digit to be ignored or repeated multiple times. Any digit (0~9, *, #) after the dot will be ignored.

  For example, (01.) means a number matching this rule can be 0, 01, 0111, 01111, and so on.
- {dialed-number:translated-number} indicates the number after the colon replaces the number before the colon in an angle bracket {}. For example,

  ({:1212} xxxxxxx) means the ZyXEL Device automatically prefixes the translated-number "1212" to the number you dialed before making the call. This can be used for local calls in the US.

  ({9:} xxx xxxxxxx) means the ZyXEL Device automatically removes the specified prefix "9" from the number you dialed before making the call. This is always used for making outside calls from an office.

  (xx{123:456}xxxx) means the ZyXEL Device automatically translates "123" to "456" in the number you dialed before making the call.
- Calls with a number followed by the exclamation mark "!" will be dropped.
- Calls with a number followed by the termination character "@" will be made immediately. Any digit (0~9, *, #) after the character will be ignored.

In this example dial plan (0 | [49]11 | 1 [2-9]xx xxxxxxx | 1 947 xxxxxxx !), you can dial "0" to call the local operator, call 411 or 911, or make a long distance call with an area code starting from 2 to 9 in the US. The calls with the area code 947 will be dropped.

9.3 The SIP Account Screen

The ZyXEL Device uses a SIP account to make outgoing VoIP calls and check if an incoming call's destination number matches your SIP account's SIP number. In order to make or receive a VoIP call, you need to enable and configure a SIP account, and map it to a phone port. The SIP account contains information that allows your ZyXEL Device to connect to your VoIP service provider.

See Section 9.4 on page 169 for how to map a SIP account to a phone port.

Use this screen to maintain basic information about each SIP account. You can also enable and disable each SIP account, configure the volume, echo cancellation and VAD (Voice Activity Detection) settings for each individual phone port on the ZyXEL Device.

Voice Activity Detection/Silence Suppression

Voice Activity Detection (VAD) detects whether or not speech is present. This lets the ZyXEL Device reduce the bandwidth that a call uses by not transmitting "silent packets" when you are not speaking.

Comfort Noise Generation

When using VAD, the ZyXEL Device generates comfort noise when the other party is not speaking. The comfort noise lets you know that the line is still connected as total silence could easily be mistaken for a lost connection.

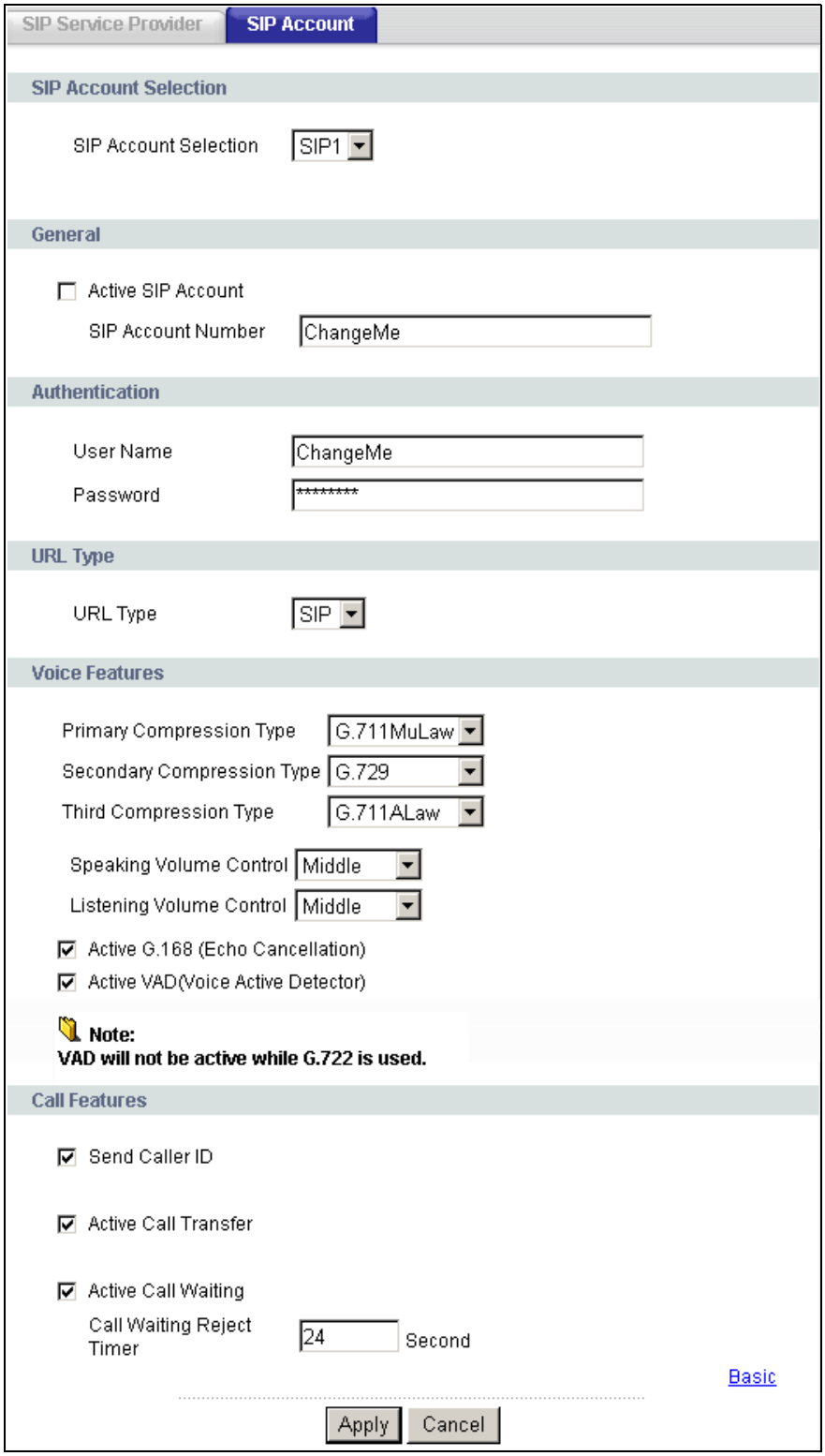
Echo Cancellation

G.168 is an ITU-T standard for eliminating the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.

To access this screen, click **VoIP > SIP > SIP Account**.

Note: Click **Advanced** to see all the fields in the screen. You don't necessarily need to use all these fields to set up your account. Click **Basic** to see and configure only the fields needed for this feature.

Figure 49 VoIP > SIP > SIP Account (Advanced)



Each field is described in the following table.

Table 38 VoIP > SIP > SIP Account

LABEL	DESCRIPTION
SIP Account Selection	
SIP Account Selection	Select the SIP account you want to see in this screen. If you change this field, the screen automatically refreshes.
General	
Active SIP Account	Select this if you want the ZyXEL Device to use this account. Clear it if you do not want the ZyXEL Device to use this account.
SIP Account Number	Enter your SIP number. In the full SIP URI, this is the part before the @ symbol. You can use up to 127 printable ASCII characters.
Authentication	
User Name	Enter the user name for registering this SIP account, exactly as it was given to you. You can use up to 95 printable ASCII characters.
Password	Enter the user name for registering this SIP account, exactly as it was given to you. You can use up to 95 printable ASCII Extended set characters.
URL Type	
URL Type	Select whether or not to include the SIP service domain name when the ZyXEL Device sends the SIP number. **SIP** - include the SIP service domain name. **TEL** - do not include the SIP service domain name.
Voice Features	
Primary Compression Type Secondary Compression Type Third Compression Type	Select the type of voice coder/decoder (codec) that you want the ZyXEL Device to use. G.711 provides higher voice quality but requires more bandwidth (64 kbps). • **G.711MuLaw** is typically used in North America and Japan. • **G.711ALaw** is typically used in Europe. • **G.729** only requires 8 kbps. • **G.726-32** operates at 16, 24, 32 or 40 kbps. **G.722** operates at 48, 56 and 64 kbps.The ZyXEL Device must use the same codec as the peer. When two SIP devices start a SIP session, they must agree on a codec. Select the ZyXEL Device's first choice for voice coder/decoder. Select the ZyXEL Device's second choice for voice coder/decoder. Select **None** if you only want the ZyXEL Device to accept the first choice. Select the ZyXEL Device's third choice for voice coder/decoder. Select **None** if you only want the ZyXEL Device to accept the first or second choice.
Speaking Volume Control	Enter the loudness that the ZyXEL Device uses for speech that it sends to the peer device. **Minimum** is the quietest, and **Maximum** is the loudest.

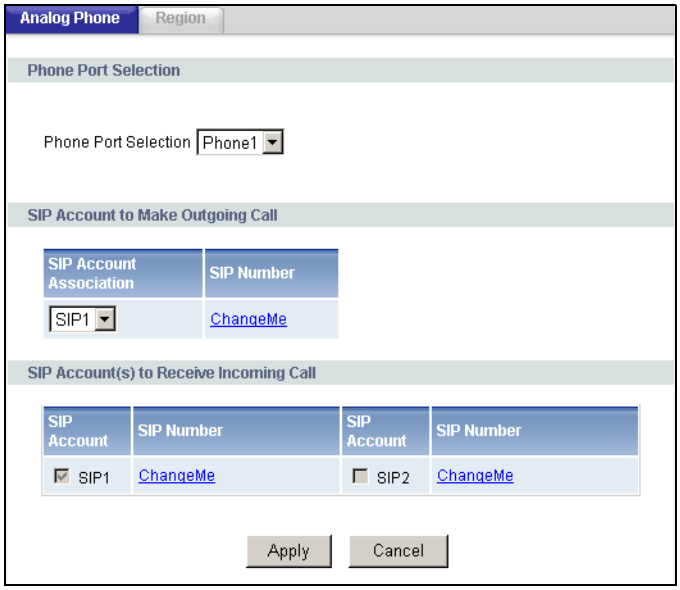
Table 38 VoIP > SIP > SIP Account

LABEL	DESCRIPTION
Listening Volume Control	Enter the loudness that the ZyXEL Device uses for speech that it receives from the peer device. **Minimum** is the quietest, and **Maximum** is the loudest.
Active G.168 (Echo Cancellation)	Select this if you want to eliminate the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.
Active VAD (Voice Active Detector)	Select this if the ZyXEL Device should stop transmitting when you are not speaking. This reduces the bandwidth the ZyXEL Device uses.
Call Features	
Send Caller ID	Select this if you want to send identification when you make VoIP phone calls. Clear this if you do not want to send identification.
Active Call Transfer	Select this to enable call transfer on the ZyXEL Device. This allows you to transfer an incoming call (that you have answered) to another phone.
Active Call Waiting	Select this to enable call waiting on the ZyXEL Device. This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.
Call Waiting Reject Timer	Specify a time of seconds that the ZyXEL Device waits before rejecting the second call if you do not answer it.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.

9.4 The Analog Phone Screen

Use this screen to control which SIP accounts and PSTN line each phone uses. To access this screen, click **VoIP > Phone > Analog Phone**.

Figure 50 VoIP > Phone > Analog Phone



Each field is described in the following table.

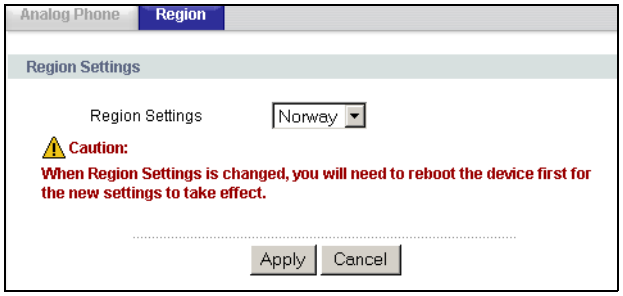
Table 39 VoIP > Phone > Analog Phone

LABEL	DESCRIPTION
Phone Port Selection	
Phone Port Selection	Select a phone port in the ZyXEL Device.
SIP Account to Make Outgoing Call	
SIP Account Association	Select the SIP account you want to use when making outgoing calls with the analog phone connected to this phone port.
SIP Number	Click this to go to a screen where you can configure the SIP number for the SIP account.
SIP Account(s) to Receive Incoming Call	
SIP Account	Select a SIP account if you want to receive phone calls for the selected SIP account on this phone port. If you select more than one SIP account for incoming calls, there is no way to distinguish between them when you receive phone calls. If you do not select a source for incoming calls, you cannot receive any calls on this phone port.
SIP Number	Click this to go to a screen where you can configure the SIP number for the SIP account.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.

9.5 The Phone Region Screen

Use this screen to maintain settings that depend on which region of the world the ZyXEL Device is in. To access this screen, click **VoIP > Phone > Region**.

Figure 51 VoIP > Phone > Region



Each field is described in the following table.

Table 40 VoIP > Phone > Region

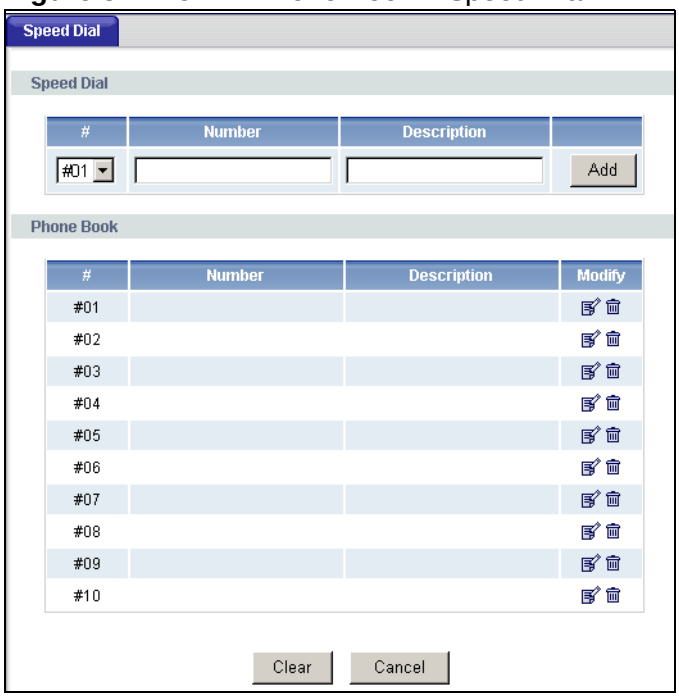
LABEL	DESCRIPTION
Region Settings	Select the place in which the ZyXEL Device is located.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.

9.6 The Speed Dial Screen

Use this screen to add, edit, or remove speed-dial numbers for outgoing calls. Speed dial provides shortcuts for dialing frequently-used (VoIP) phone numbers. You also have to create speed-dial entries if you want to call SIP numbers that contain letters. Once you have configured a speed dial rule, you can use a shortcut (the speed dial number, #01 for example) on your phone's keypad to call the phone number.

To access this screen, click **VoIP > Phonebook > Speed Dial**.

Figure 52 VoIP > Phone Book > Speed Dial



Each field is described in the following table.

Table 41 VoIP > Phone Book > Speed Dial

LABEL	DESCRIPTION
Speed Dial	Use this section to create or edit speed-dial entries.
#	Select the speed-dial number you want to use for this phone number.
Number	Enter the SIP number you want the ZyXEL Device to call when you dial the speed-dial number.
Description	Enter a short description to identify the party you call when you dial the speed-dial number. You can use up to 127 printable ASCII characters.
Add	Click this to use the information in the **Speed Dial** section to update the **Speed Dial Phone Book** section.
Phone Book	Use this section to look at all the speed-dial entries and to erase them.
#	This field displays the speed-dial number you should dial to use this entry.
Number	This field displays the SIP number the ZyXEL Device calls when you dial the speed-dial number.
Description	This field displays a short description of the party you call when you dial the speed-dial number.
Modify	Use this field to edit or erase the speed-dial entry. Click the **Edit** icon to copy the information for this speed-dial entry into the **Speed Dial** section, where you can change it. Click the **Remove** icon to erase this speed-dial entry.

Table 41 VoIP > Phone Book > Speed Dial

LABEL	DESCRIPTION
Clear	Click this to erase all the speed-dial entries.
Cancel	Click this to set every field in this screen to its last-saved value.

9.7 SIP Technical Reference

This section contains background material relevant to the **VoIP** screens.

9.7.1 VoIP

VoIP is the sending of voice signals over Internet Protocol. This allows you to make phone calls and send faxes over the Internet at a fraction of the cost of using the traditional circuit-switched telephone network. You can also use servers to run telephone service applications like PBX services and voice mail. Internet Telephony Service Provider (ITSP) companies provide VoIP service.

Circuit-switched telephone networks require 64 kilobits per second (Kbps) in each direction to handle a telephone call. VoIP can use advanced voice coding techniques with compression to reduce the required bandwidth.

9.7.2 SIP

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet.

SIP signaling is separate from the media for which it handles sessions. The media that is exchanged during the session can use a different path from that of the signaling. SIP handles telephone calls and can interface with traditional circuit-switched telephone networks.

SIP Identities

A SIP account uses an identity (sometimes referred to as a SIP address). A complete SIP identity is called a SIP URI (Uniform Resource Identifier). A SIP account's URI identifies the SIP account in a way similar to the way an e-mail address identifies an e-mail account. The format of a SIP identity is SIP-Number@SIP-Service-Domain.

SIP Number

The SIP number is the part of the SIP URI that comes before the “@” symbol. A SIP number can use letters like in an e-mail address (johndoe@your-ITSP.com for example) or numbers like a telephone number (1122334455@VoIP-provider.com for example).

SIP Service Domain

The SIP service domain of the VoIP service provider is the domain name in a SIP URI. For example, if the SIP address is 1122334455@VoIP-provider.com, then “VoIP-provider.com” is the SIP service domain.

SIP Registration

Each ZyXEL Device is an individual SIP User Agent (UA). To provide voice service, it has a public IP address for SIP and RTP protocols to communicate with other servers.

A SIP user agent has to register with the SIP registrar and must provide information about the users it represents, as well as its current IP address (for the routing of incoming SIP requests). After successful registration, the SIP server knows that the users (identified by their dedicated SIP URIs) are represented by the UA, and knows the IP address to which the SIP requests and responses should be sent.

Registration is initiated by the User Agent Client (UAC) running in the VoIP gateway (the ZyXEL Device). The gateway must be configured with information letting it know where to send the REGISTER message, as well as the relevant user and authorization data.

A SIP registration has a limited lifespan. The User Agent Client must renew its registration within this lifespan. If it does not do so, the registration data will be deleted from the SIP registrar's database and the connection broken.

The ZyXEL Device attempts to register all enabled subscriber ports when it is switched on. When you enable a subscriber port that was previously disabled, the ZyXEL Device attempts to register the port immediately.

Authorization Requirements

SIP registrations (and subsequent SIP requests) require a username and password for authorization. These credentials are validated via a challenge / response system using the HTTP digest mechanism (as detailed in RFC3261, "SIP: Session Initiation Protocol").

SIP Servers

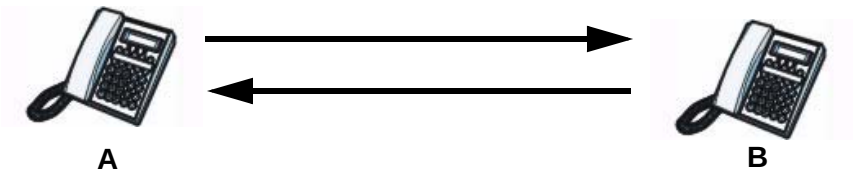
SIP is a client-server protocol. A SIP client is an application program or device that sends SIP requests. A SIP server responds to the SIP requests.

When you use SIP to make a VoIP call, it originates at a client and terminates at a server. A SIP client could be a computer or a SIP phone. One device can act as both a SIP client and a SIP server.

SIP User Agent

A SIP user agent can make and receive VoIP telephone calls. This means that SIP can be used for peer-to-peer communications even though it is a client-server protocol. In the following figure, either **A** or **B** can act as a SIP user agent client to initiate a call. **A** and **B** can also both act as a SIP user agent to receive the call.

Figure 53 SIP User Agent



SIP Proxy Server

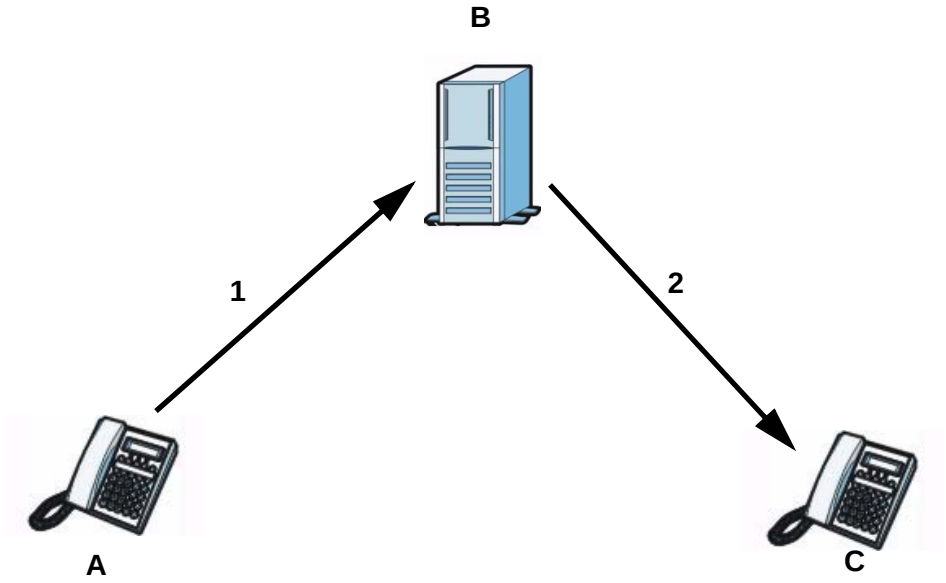
A SIP proxy server receives requests from clients and forwards them to another server.

In the following example, you want to use client device **A** to call someone who is using client device C.

1 The client device (**A** in the figure) sends a call invitation to the SIP proxy server (**B**).

2 The SIP proxy server forwards the call invitation to **C**.

Figure 54 SIP Proxy Server



SIP Redirect Server

A SIP redirect server accepts SIP requests, translates the destination address to an IP address and sends the translated IP address back to the device that sent the request. Then the client device that originally sent the request can send requests to the IP address that it received back from the redirect server. Redirect servers do not initiate SIP requests.

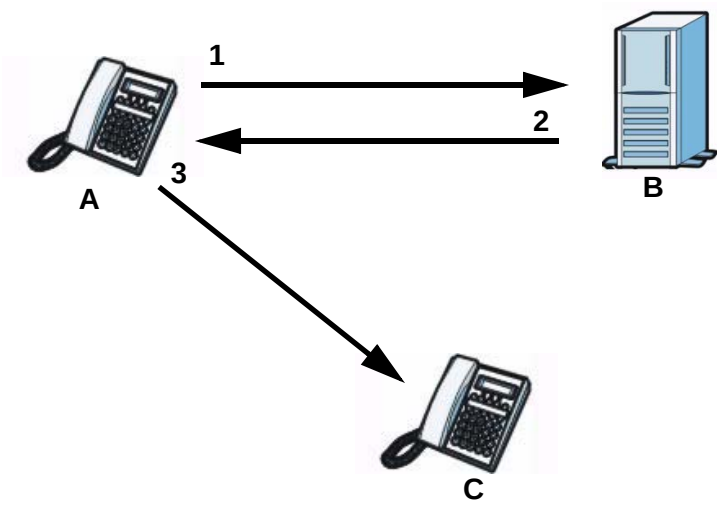
In the following example, you want to use client device **A** to call someone who is using client device **C**.

1 Client device **A** sends a call invitation for **C** to the SIP redirect server (**B**).

2 The SIP redirect server sends the invitation back to **A** with **C**'s IP address (or domain name).

3 Client device **A** then sends the call invitation to client device **C**.

Figure 55 SIP Redirect Server



SIP Register Server

A SIP register server maintains a database of SIP identity-to-IP address (or domain name) mapping. The register server checks your user name and password when you register.

RTP

When you make a VoIP call using SIP, the RTP (Real time Transport Protocol) is used to handle voice data transfer. See RFC 1889 for details on RTP.

Pulse Code Modulation

Pulse Code Modulation (PCM) measures analog signal amplitudes at regular time intervals and converts them into bits.

SIP Call Progression

The following figure displays the basic steps in the setup and tear down of a SIP call. A calls B.

Table 42 SIP Call Progression

A		B
1. INVITE	→	
	←	2. Ringing
	←	3. OK
4. ACK	→	

Table 42 SIP Call Progression (continued)

A		B
	5.Dialogue (voice traffic)	
6. BYE		
		7. OK

1 **A** sends a SIP INVITE request to **B**. This message is an invitation for **B** to participate in a SIP telephone call.

2 **B** sends a response indicating that the telephone is ringing.

3 **B** sends an OK response after the call is answered.

4 **A** then sends an ACK message to acknowledge that **B** has answered the call.

5 Now **A** and **B** exchange voice media (talk).

6 After talking, **A** hangs up and sends a BYE request.

7 **B** replies with an OK response confirming receipt of the BYE request and the call is terminated.

Voice Coding

A codec (coder/decoder) codes analog voice signals into digital signals and decodes the digital signals back into analog voice signals. The ZyXEL Device supports the following codecs.

- G.711 is a Pulse Code Modulation (PCM) waveform codec. PCM measures analog signal amplitudes at regular time intervals and converts them into digital samples. G.711 provides very good sound quality but requires 64 kbps of bandwidth.
- G.726 is an Adaptive Differential PCM (ADPCM) waveform codec that uses a lower bitrate than standard PCM conversion. ADPCM converts analog audio into digital signals based on the difference between each audio sample and a prediction based on previous samples. The more similar the audio sample is to the prediction, the less space needed to describe it. G.726 operates at 16, 24, 32 or 40 kbps.
- G.729 is an Analysis-by-Synthesis (AbS) hybrid waveform codec that uses a filter based on information about how the human vocal tract produces sounds. G.729 provides good sound quality and reduces the required bandwidth to 8 kbps.

PSTN Call Setup Signaling

Dual-Tone MultiFrequency (DTMF) signaling uses pairs of frequencies (one lower frequency and one higher frequency) to set up calls. It is also known as Touch Tone®. Each of the keys on a DTMF telephone corresponds to a different pair of frequencies.

Pulse dialing sends a series of clicks to the local phone office in order to dial numbers.[1]

MWI (Message Waiting Indication)

Enable Message Waiting Indication (MWI) enables your phone to give you a message–waiting (beeping) dial tone when you have a voice message(s). Your VoIP service provider must have a messaging system that sends message waiting status SIP packets as defined in RFC 3842.

9.7.3 Quality of Service (QoS)

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to provide bandwidth for real-time multimedia applications.

Type of Service (ToS)

Network traffic can be classified by setting the ToS (Type of Service) values at the data source (for example, at the ZyXEL Device) so a server can decide the best method of delivery, that is the least cost, fastest route and so on.

DiffServ

DiffServ is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCP) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.[2]

1. The ZyXEL Device does not support pulse dialing at the time of writing.
2. The ZyXEL Device does not support DiffServ at the time of writing.

DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

Figure 56 DiffServ: Differentiated Service Field

DSCP (6-bit)	Unused (2-bit)

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different priorities of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

VLAN Tagging

Virtual Local Area Network (VLAN) allows a physical network to be partitioned into multiple logical networks. Only stations within the same group can communicate with each other.

Your ZyXEL Device can add IEEE 802.1Q VLAN ID tags to voice frames that it sends to the network. This allows the ZyXEL Device to communicate with a SIP server that is a member of the same VLAN group. Some ISPs use the VLAN tag to identify voice traffic and give it priority over other traffic.

9.7.4 Phone Services Overview

Supplementary services such as call hold, call waiting, and call transfer. are generally available from your VoIP service provider. The ZyXEL Device supports the following services:

- Call Hold
- Call Waiting
- Making a Second Call
- Call Transfer
- Three-Way Conference

- Internal Calls
- Call Park and Pickup
- Do not Disturb

Note: To take full advantage of the supplementary phone services available through the ZyXEL Device's phone ports, you may need to subscribe to the services from your VoIP service provider.

The Flash Key

Flashing means to press the hook for a short period of time (a few hundred milliseconds) before releasing it. On newer telephones, there should be a "flash" key (button) that generates the signal electronically. If the flash key is not available, you can tap (press and immediately release) the hook by hand to achieve the same effect. However, using the flash key is preferred since the timing is much more precise. With manual tapping, if the duration is too long, it may be interpreted as hanging up by the ZyXEL Device.

You can invoke all the supplementary services by using the flash key.

Europe Type Supplementary Phone Services

This section describes how to use supplementary phone services with the **Europe Type Call Service Mode**. Commands for supplementary services are listed in the table below.

After pressing the flash key, if you do not issue the sub-command before the default sub-command timeout (2 seconds) expires or issue an invalid sub-command, the current operation will be aborted.

Table 43 European Flash Key Commands

COMMAND	SUB-COMMAND	DESCRIPTION
Flash		Put a current call on hold to place a second call. Switch back to the call (if there is no second call).
Flash	0	Drop the call presently on hold or reject an incoming call which is waiting for answer.
Flash	1	Disconnect the current phone connection and answer the incoming call or resume with caller presently on hold.
Flash	2	1. Switch back and forth between two calls. 2. Put a current call on hold to answer an incoming call. 3. Separate the current three-way conference call into two individual calls (one is on-line, the other is on hold).
Flash	3	Create three-way conference connection.
Flash	*98#	Transfer the call to another phone.

European Call Hold

Call hold allows you to put a call (**A**) on hold by pressing the flash key.

If you have another call, press the flash key and then “2” to switch back and forth between caller **A** and **B** by putting either one on hold.

Press the flash key and then “0” to disconnect the call presently on hold and keep the current call on line.

Press the flash key and then “1” to disconnect the current call and resume the call on hold.

If you hang up the phone but a caller is still on hold, there will be a remind ring.

European Call Waiting

This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

If there is a second call to a telephone number, you will hear a call waiting tone. Take one of the following actions.

- Reject the second call.

  Press the flash key and then press “0”.
- Disconnect the first call and answer the second call.

  Either press the flash key and press “1”, or just hang up the phone and then answer the phone after it rings.
- Put the first call on hold and answer the second call.

  Press the flash key and then “2”.

European Call Transfer

Do the following to transfer an incoming call (that you have answered) to another phone.

1 Press the flash key to put the caller on hold.

2 When you hear the dial tone, dial “*98#” followed by the number to which you want to transfer the call. to operate the Intercom.

3 After you hear the ring signal or the second party answers it, hang up the phone.

European Three-Way Conference

Use the following steps to make three-way conference calls.

1. When you are on the phone talking to someone, press the flash key to put the caller on hold and get a dial tone.
2. Dial a phone number directly to make another call.
3. When the second call is answered, press the flash key and press “3” to create a three-way conversation.
4. Hang up the phone to drop the connection.
5. If you want to separate the activated three-way conference into two individual connections (one is on-line, the other is on hold), press the flash key and press “2”.

10

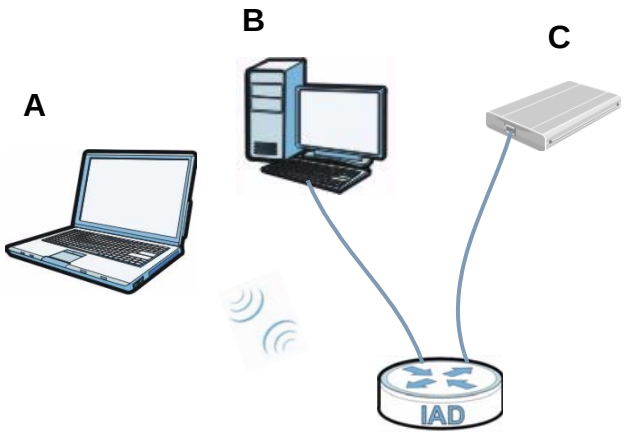
File Sharing

10.1 Overview

Share files on a USB memory stick or hard drive connected to your ZyXEL Device with users on your network.

The following figure is an overview of the ZyXEL Device's file server feature. Computers **A** and **B** can access files on a USB device (**C**) which is connected to the ZyXEL Device.

Figure 57 File Sharing Overview



- See Section 10.1.2 on page 184 for an explanation of file sharing terms.
- See Section 3.6 on page 50 for a file sharing tutorial.

10.1.1 What You Can Do in this Chapter

- Use the **Share Configuration** screen (Section 10.2 on page 185) to enable file sharing server on the ZyXEL Device and configure the workgroup name.
- Use the **Account Management** screen (Section 10.3 on page 190) to set up and configure a file sharing account.

10.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter.

User Account

This gives you access to the file sharing server. It includes your user name and password.

Workgroup name

This is the name given to a set of computers that are connected on a network and share resources such as a printer or files. Windows automatically assigns the workgroup name when you set up a network.

Shares

When settings are set to default, each USB device connected to the ZyXEL Device is given a folder, called a “share”. If a USB hard drive connected to the ZyXEL Device has more than one partition, then each partition will be allocated a share. You can also configure a “share” to be a sub-folder or file on the USB device.

File Systems

A file system is a way of storing and organizing files on your hard drive and storage device. Often different operating systems such as Windows or Linux have different file systems. The file sharing feature on your ZyXEL Device supports File Allocation Table (FAT), FAT32, and New Technology File System (NTFS).

Common Internet File System

The ZyXEL Device uses Common Internet File System (CIFS) protocol for its file sharing functions. CIFS compatible computers can access the USB file storage devices connected to the ZyXEL Device. CIFS protocol is supported on Microsoft Windows, Linux Samba and other operating systems (refer to your systems specifications for CIFS compatibility).

10.1.3 Before You Begin

Make sure the ZyXEL Device is connected to your network and turned on.

1 Connect the USB device to one of the ZyXEL Device’s USB ports. Make sure the ZyXEL Device is connected to your network.

2 The ZyXEL Device detects the USB device and makes its contents available for browsing. If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.

Note: If your USB device cannot be detected by ZyXEL Device, see the troubleshooting for suggestions.

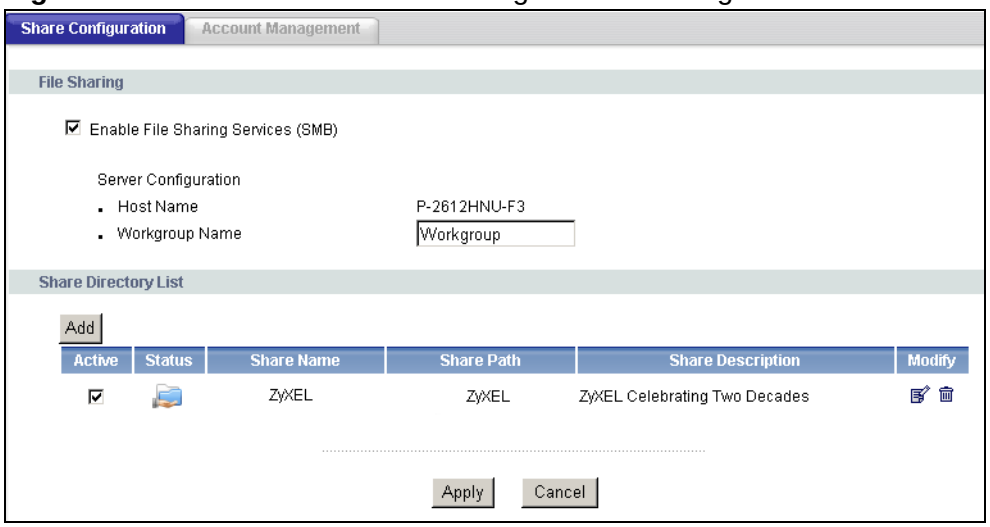
10.2 The Share Configuration Screen

In the **Server Settings** screen you need to configure your ZyXEL Device's **Workgroup Name**.

The ZyXEL Device will not be able to join the workgroup if your local area network has restrictions set up that do not allow devices to join a workgroup. In this case, contact your network administrator.

Use this screen to set up file sharing using the ZyXEL Device. To access this screen, click **USB Services > File Sharing**.

Figure 58 USB Services > File Sharing > Share Configuration



Each field is described in the following table.

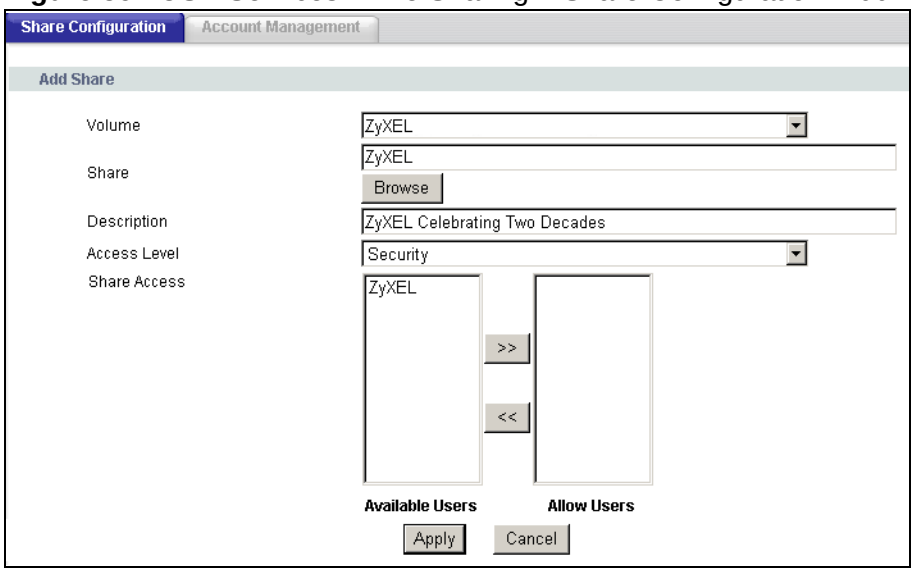
Table 44 USB Services > File Sharing > Share Configuration

LABEL	DESCRIPTION
Enable File Sharing Services (SMB)	Select this to enable file sharing through the ZyXEL Device.
Server Configuration	
Host Name	This shows the read-only name that identifies the ZyXEL Device in your network. You can change this in the **Maintenance > System** screen.
Workgroup Name	You can add the ZyXEL Device to an existing or a new workgroup on your network. Enter the name of the workgroup which your ZyXEL Device automatically joins. You can set the ZyXEL Device's workgroup name to be exactly the same as the workgroup name to which your computer belongs.
Share Directory List	These fields identify the shares configured on the ZyXEL Device. Note: You must connect a USB storage device to the ZyXEL Device in order to see this section of the screen.
Add	Click this to set up a new share on the ZyXEL Device. See Section 10.2.1 on page 187.
Active	Check this to make the share available to the network. Otherwise, clear this.
Status	This shows whether or not the share is available for sharing.
Share Name	This field displays the share name on the ZyXEL Device.
Share Path	This field displays the path for the share directories (folders) on the ZyXEL Device. These are the directories (folders) on your USB storage device.
Share Description	This field displays information about the share. You can add share descriptions to shares in the **Share Configuration Add/Edit** screen (see Section 10.2.1 on page 187 and Section 10.2.2 on page 189).
Modify	Click the **Edit** icon to change the settings of an existing share. See Section 10.2.2 on page 189. Click the **Remove** icon to delete this share in the list. You will be asked to confirm this action.
Apply	Click this to save your changes to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.

10.2.1 Share Configuration Add Screen

Use this screen to set up a new share on the ZyXEL Device. Click **Add** in the **USB Services > File Sharing > Share Configuration** screen.

Figure 59 USB Services > File Sharing > Share Configuration: Add



Each field is described in the following table.

Table 45 USB Services > File Sharing > Share Configuration: Add

LABEL	DESCRIPTION
Volume	Select the volume in the USB storage device that you want to add as a share in the ZyXEL Device.
Share	Manually enter the file path for the share, or click the **Browse** button. Refer to Section 10.2.1.1 on page 188 to see the **Browse** screen.
Browse	Click this button to select the file path for the share directory. This is the folder that will be visible to a user browsing to the USB storage device. A user can access any sub-folder in this folder.
Description	You can either enter a short description of the share, or leave this field blank.
Access Level	The share can either be available to everyone in the network or only to users you add in the **Account Management** screen. Select **Public** to make the share available to everyone. Select **Security** to make the share available only to users you allow.
Share Access	This shows when you select **Security** as the **Access Level** for the share. You can allow or disallow access simply by moving **Available Users** to the **Allow Users** box.

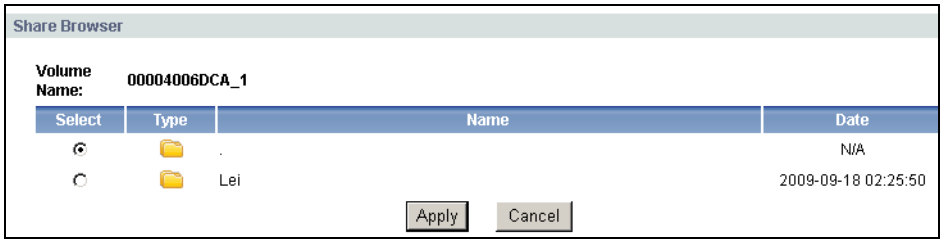
Table 45 USB Services > File Sharing > Share Configuration: Add

LABEL	DESCRIPTION
Apply	Click this button to save your settings.
Cancel	Click this button to return all fields in this screen to their previous values.

10.2.1.1 Share Configuration Browse Screen

To select the file path for the share directory, click **Browse** in the previous screen.

Figure 60 USB Services > File Sharing > Share Configuration: Browse



Each field is described in the following table.

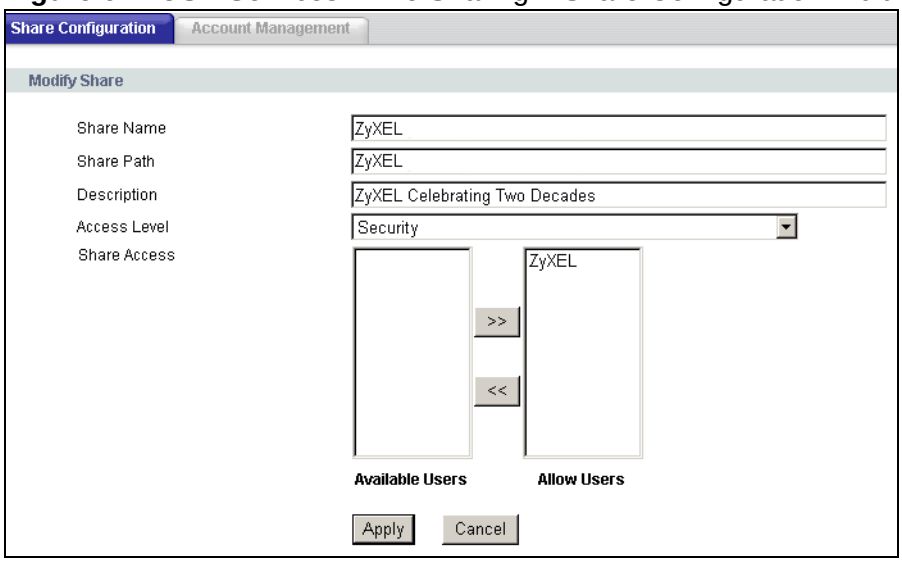
Table 46 USB Services > File Sharing > Share Configuration: Browse

LABEL	DESCRIPTION
Volume Name	This shows the volume in the USB storage device that was added as a share in the ZyXEL Device.
The table below shows the folders that are currently in the USB storage device that you have connected to the ZyXEL Device.	
Select	Click the folder that you want to add as a share in the ZyXEL Device.
Type	This shows an icon representing the folders in the USB storage device.
Name	This displays the name of the folder in the current directory of the connected USB storage device. Click on a folder name to add that folder to the directory path for the share. '.' shows the current directory of the USB storage device.
Date	This shows the date when the folder was last available.
Apply	Click this button to save your settings.
Cancel	Click this button to return all fields in this screen to their previous values.

10.2.2 Share Configuration Edit Screen

Use this screen to edit an existing share on the ZyXEL Device. Click **Edit** in the **USB Services > File Sharing > Share Configuration** screen.

Figure 61 USB Services > File Sharing > Share Configuration: Edit



Each field is described in the following table.

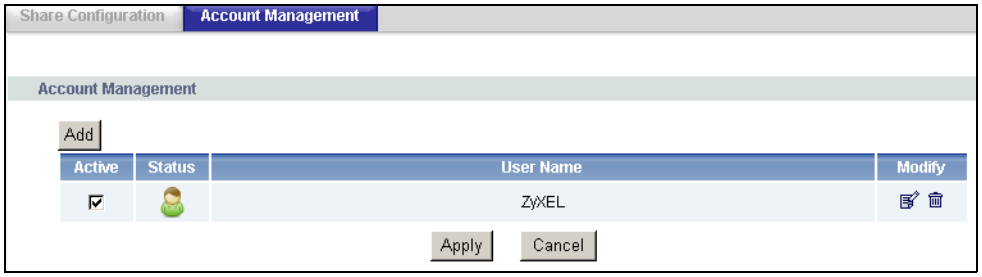
Table 47 USB Services > File Sharing > Share Configuration: Edit

LABEL	DESCRIPTION
Share Name	Manually enter the share name on the ZyXEL Device.
Share Path	This field displays the directory (folder) used for the share on your USB storage device. It is non-configurable when you edit an existing share.
Description	Enter a short description or some information about the share.
Access Level	The share can either be available to everyone in the network or only to users you add in the **Account Management** screen. Select **Public** to make the share available to everyone. Select **Security** to make the share available only to users you allow.
Share Access	This shows when you select **Security** as the **Access Level** for the share. You can allow or disallow access simply by moving **Available Users** to the **Allow Users** box.
Apply	Click this button to save your settings.
Cancel	Click this button to return all fields in this screen to their previous values.

10.3 The Account Management Screen

Use this screen to configure a user account. To access this screen, click **USB Services > File Sharing > Account Management**.

Figure 62 USB Services > File Sharing > Account Management



Each field is described in the following table.

Table 48 USB Services > File Sharing > Account Management

LABEL	DESCRIPTION
Add	Click this button to configure another user and include it in the list.
Active	Check this to enable the user to access shares via the ZyXEL Device. Otherwise clear this to prevent this user from accessing shares via the ZyXEL Device.
Status	This shows whether the user name is active (able to access shares via the ZyXEL Device) or inactive (unable to access shares via the ZyXEL Device).
User Name	This field shows the list of user names already configured on the ZyXEL Device.
Modify	Click the **Edit** icon to change the settings of an existing user account. Click the **Remove** icon to delete this entry in the list. You will be asked to confirm this action.

10.3.1 Account Management Add or Edit Screen

Use the following screens to add or edit a user account. To access these screens, click **Advanced > File Sharing > User Configuration** and click the **Add** button or the **Edit** icon in the **Modify** column or the **Add** button.

Figure 63 USB Services > File Sharing > Account Management > Add

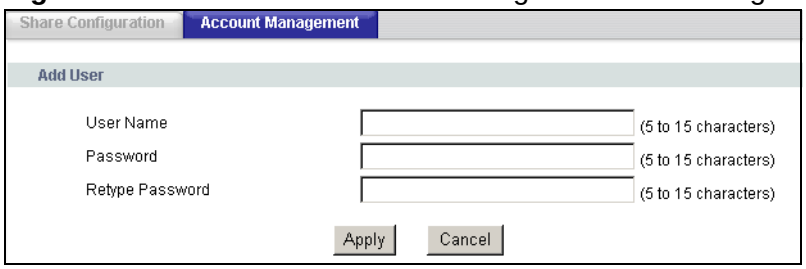
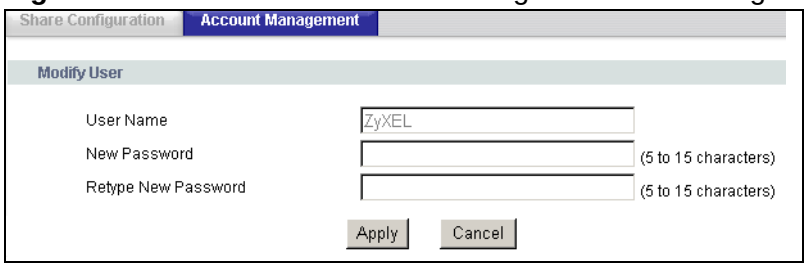


Figure 64 USB Services > File Sharing > Account Management > Edit



Each field is described in the following table.

Table 49 USB Services > File Sharing > Account Management > Add/Edit

LABEL	DESCRIPTION
User Name	This field is not configurable if you click the Edit icon in the **Modify** column to configure an existing user account. Enter the user name of the account. The user name can be 5 to 15 alpha-numeric characters long.
New Password/ Password	Enter the password for this account. The password can be 5 to 15 alpha-numeric characters long.
Retype New Password/ Retype Password	Retype the password.
Apply	Click this to save your changes to the ZyXEL Device.
Reset	Click this to set the fields in this screen to their defaults.

11

Media Server

11.1 Overview

The media server feature lets anyone on your network play video, music, and photos from the USB storage device connected to your ZyXEL Device (without having to copy them to another computer). The ZyXEL Device can function as a DLNA-compliant media server. The ZyXEL Device streams files to DLNA-compliant media clients (like Windows Media Player). The Digital Living Network Alliance (DLNA) is a group of personal computer and electronics companies that works to make products compatible in a home network.

11.1.1 What You Can Do

Use the **Media Server** screen (Section 11.2 on page 194) to enable or disable the sharing of media files.

11.1.2 What You Need to Know in this Chapter

The ZyXEL Device media server enables you to:

- Publish all shares for everyone to play media files in the USB storage device connected to the ZyXEL Device.
- Use hardware-based media clients like the DMA-2500 to play the files.

Note: Anyone on your network can play the media files in the published shares. No user name and password or other form of security is used. The media server is enabled by default with the video, photo, and music shares published.

11.2 The Media Server Screen

To change your ZyXEL Device's media server settings, click **USB Services** > **Media Server**. The screen appears as shown.

Figure 65 USB Services > Media Server

The following table describes the labels in this menu.

Table 50 USB Services > Media Server

LABEL	DESCRIPTION
Enable Media Server	Check this to have the ZyXEL Device function as a DLNA-compliant media server. Turn on the media server to let (DLNA-compliant) media clients on your network play media files located in the shares. Otherwise, clear this.
Apply	Click this to save your changes back to the ZyXEL Device.
Cancel	Click this to reload the previous configuration for this screen.

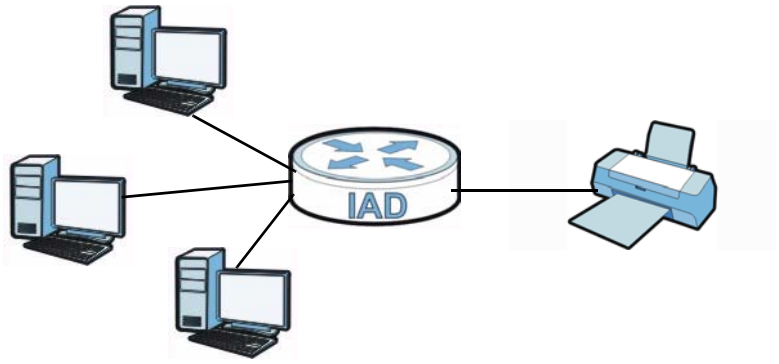
12 Print Server

12.1 Overview

This chapter describes how you can share a USB printer via your ZyXEL Device.

The ZyXEL Device allows you to share a USB printer on your LAN. You can do this by connecting a USB printer to one of the USB ports on the ZyXEL Device and then configuring a TCP/IP port on the computers connected to your network.

Figure 66 Sharing a USB Printer



12.1.1 What You Can Do in this Chapter

Use the **Print Server** screen (Section 12.2 on page 197) to enable or disable sharing of a USB printer via your ZyXEL Device.

12.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter.

Print Server

This is a computer or other device which manages one or more printers, and which sends print jobs to each printer from the computer itself or other devices.

Operating System

An operating system (OS) is the interface which helps you manage a computer. Common examples are Microsoft Windows, Mac OS or Linux.

TCP/IP

TCP/IP (Transmission Control Protocol/ Internet Protocol) is a set of communications protocols that most of the Internet runs on.

Port

A port maps a network service such as http to a process running on your computer, such as a process run by your web browser. When traffic from the Internet is received on your computer, the port number is used to identify which process running on your computer it is intended for.

Line Printer Remote Protocol

The Line Printer Remote (LPR) Protocol is software that provides printer spooling and print-server features using TCP/IP to connect printers and computers on a network.

Supported OSs

Your operating system must support TCP/IP ports for printing and be compatible with the LPR protocol.

The following OSs support ZyXEL Device's printer sharing feature.

- Microsoft Windows 95, Windows 98 SE (Second Edition), Windows Me, Windows NT 4.0, Windows 2000, Windows XP or Macintosh OS X.

12.1.3 Before You Begin

To configure the print server you need the following:

- Your ZyXEL Device must be connected to your computer and any other devices on your network. The USB printer must be connected to your ZyXEL Device.
- A USB printer with the driver already installed on your computer.
- The computers on your network must have the printer software already installed before they can create a TCP/IP port for printing via the network. Follow your printer manufacturers instructions on how to install the printer software on your computer.

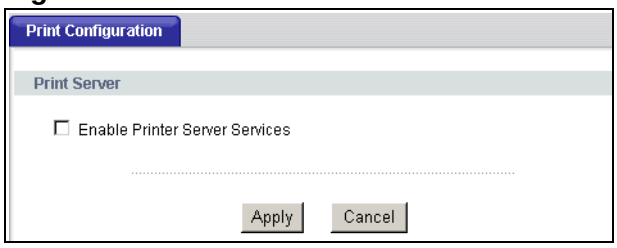
Note: Your printer's installation instructions may ask that you connect the printer to your computer. Connect your printer to the ZyXEL Device instead.

12.2 The Print Server Screen

Use this screen to enable or disable sharing of a USB printer via your ZyXEL Device.

To access this screen, click **USB Services > Print Server**.

Figure 67 USB Services > Print Server



The following table describes the labels in this menu.

Table 51 USB Services > Print Server

LABEL	DESCRIPTION
Enable Printer Server Services	Check this to have the ZyXEL Device share a USB printer. Otherwise, clear this.
Apply	Click this to save your changes back to the ZyXEL Device.
Cancel	Click this to reload the previous configuration for this screen.

12.3 Technical Reference

The following section contains additional technical information about the ZyXEL Device features described in this chapter.

ZyXEL Device Print Server Compatible USB Printers

The following is a list of USB printer models compatible with the ZyXEL Device print server.

Table 52 Compatible USB Printers

BRAND	MODEL
Brother	MFC7420
CANON	BJ F9000
CANON	i320
CANON	PIXMA MP450

Table 52 Compatible USB Printers (continued)

BRAND	MODEL
CANON	PIXMA MP730
CANON	PIXMA MP780
CANON	PIXMA MP830
CANON	PIXUS ip2500
CANON	PIXMA ip4200
CANON	PIXMA ip5000
CANON	PIXUS 990i
EPSON	CX3500
EPSON	CX3900
EPSON	EPL-5800
EPSON	EPL-6200L
EPSON	LP-2500
EPSON	LP-8900
EPSON	RX 510
EPSON	RX 530
EPSON	Stylus 830U
EPSON	Stylus 1270
EPSON	Stylus C43UX
EPSON	Stylus C60
EPSON	Stylus Color 670
HP	Deskjet 5550
HP	Deskjet 5652
HP	Deskjet 830C
HP	Deskjet 845C
HP	Deskjet 1125C
HP	Deskjet 1180C
HP	Deskjet 1220C
HP	Deskjet F4185
HP	Laserjet 1022
HP	Laserjet 1200
HP	Laserjet 2200D
HP	Laserjet 2420

Table 52 Compatible USB Printers (continued)

BRAND	MODEL
HP	Color Laserjet 1500L
HP	Laserjet 3015
HP	Officejet 4255
HP	Officejet 5510
HP	Officejet 5610
HP	Officejet 7210
HP	Officejet Pro L7380
HP	Photosmart 2610
HP	Photosmart 3110
HP	Photosmart 7150
HP	Photosmart 7830
HP	Photosmart C5280
HP	Photosmart D5160
HP	PSC 1350
HP	PSC 1410
IBM	Infoprint 1332
LEXMARK	Z55
LEXMARK	Z705
OKI	B4350
SAMSUNG	ML-1710
SAMSUNG	SCX-4016

13

MAC Filter

13.1 Overview

This chapter discusses MAC address filtering.

The MAC filter screen allows you to configure the ZyXEL Device to give exclusive access to up to 32 wireless clients (Allow) based on the MAC address of the wireless clients.

This applies to wired and wireless connections.

13.1.1 What You Can Do in this Chapter

Use the **MAC Filter** screen (Section 13.2 on page 202) to allow wireless clients access to the ZyXEL Device.

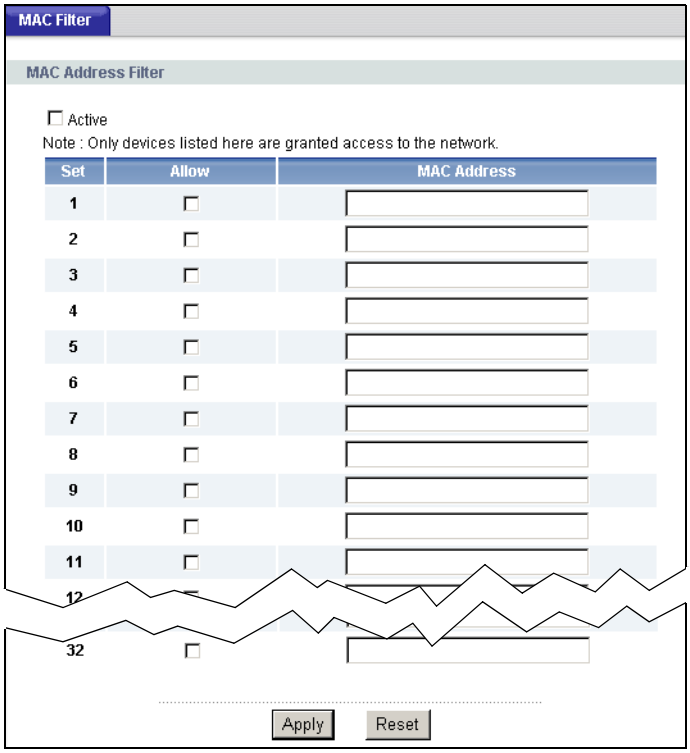
13.1.2 What You Need to Know

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of the devices to configure this screen.

13.2 MAC Filter Screen

To change your ZyXEL Device's MAC filter settings, click **Security** > **MAC Filter**. The screen appears as shown.

Figure 68 Security > MAC Filter



The following table describes the labels in this menu.

Table 53 Security > MAC Filter

LABEL	DESCRIPTION
Active	Check this to enable MAC address filtering.
Set	This is the index number of the MAC address.
Allow	Select **Allow** to permit access to the ZyXEL Device. MAC addresses not listed will be denied access to the ZyXEL Device. If you clear this, the **MAC Address** field for this set clears.
MAC Address	Enter the MAC addresses of the wireless station that are allowed access to the ZyXEL Device in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to reload the previous configuration for this screen.

14 Firewall

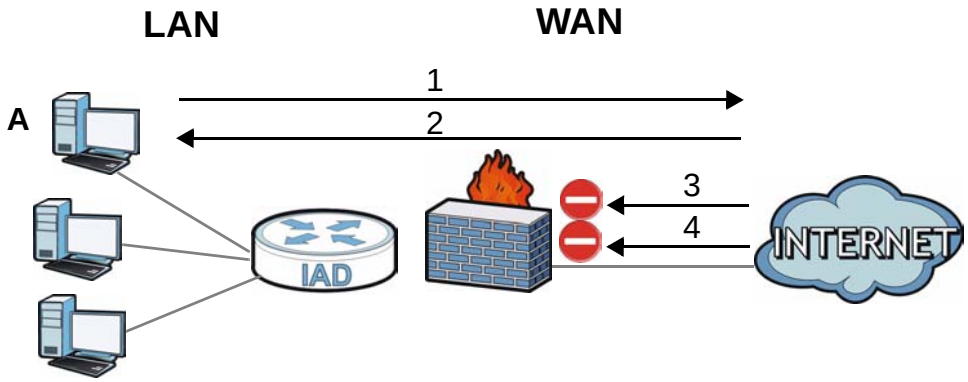
14.1 Overview

Use the ZyXEL Device firewall screens to enable and configure the firewall that protects your ZyXEL Device and network from attacks by hackers on the Internet and control access to it. By default the firewall:

- allows traffic that originates from your LAN computers to go to all other networks.
- blocks traffic that originates on other networks from going to the LAN.

The following figure illustrates the default firewall action. User **A** can initiate an IM (Instant Messaging) session from the LAN to the WAN (**1**). Return traffic for this session is also allowed (**2**). However other traffic initiated from the WAN is blocked (**3** and **4**).

Figure 69 Default Firewall Action



14.1.1 What You Can Do in the Firewall Screens

Use the **Firewall** screen (Section 14.2 on page 204) to enable LAN-to-WAN services blocking on the ZyXEL Device.

14.1.2 What You Need to Know About Firewall

The following terms and concepts may help as you read this chapter.

DoS

Denials of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources. The ZyXEL Device is pre-configured to automatically detect and thwart all known DoS attacks.

Anti-Probing

If an outside user attempts to probe an unsupported port on your ZyXEL Device, an ICMP response packet is automatically returned. This allows the outside user to know the ZyXEL Device exists. The ZyXEL Device supports anti-probing, which prevents the ICMP response packet from being sent. This keeps outsiders from discovering your ZyXEL Device when unsupported ports are probed.

ICMP

Internet Control Message Protocol (ICMP) is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.

Finding Out More

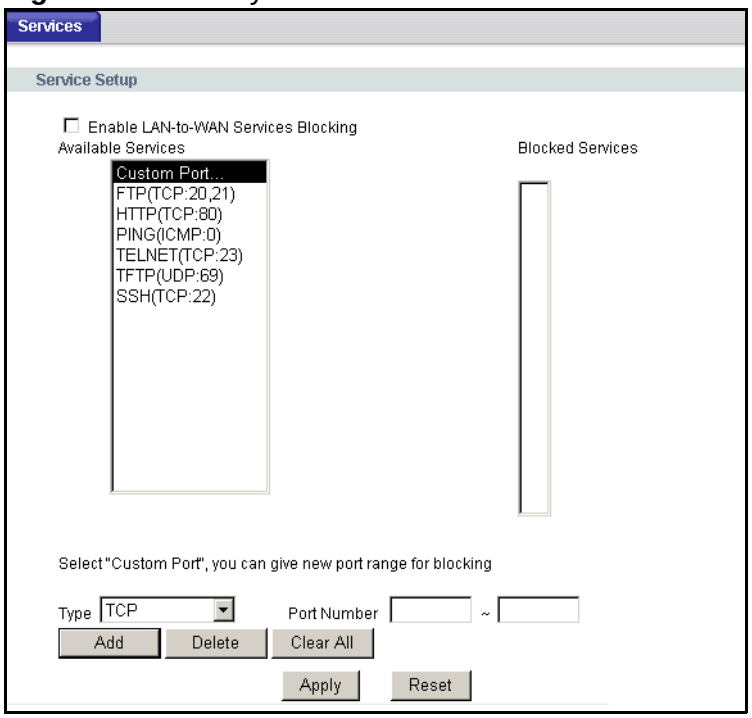
See Section 14.3 on page 206 for advanced technical information on firewall.

14.2 The Firewall Screen

Use this screen to enable service blocking and to maintain the list of services you want to block. To access this screen, click **Security > Firewall**.

Note: These rules specify which computers on the LAN can access which computers or services on the WAN.

Figure 70 Security > Firewall



Each field is described in the following table.

Table 54 Security > Firewall

LABEL	DESCRIPTION
Enable LAN-to-WAN Services Blocking	Select this to activate service blocking.
Available Services	This is a list of pre-defined services (destination ports) you may prohibit your LAN computers from using. Select the port you want to block, and click **Add** to add the port to the **Blocked Services** field. A custom port is a service that is not available in the pre-defined **Available Services** list. You must define it using the **Type** and **Port Number** fields. See Appendix E on page 369 for some examples of services.
Blocked Services	This is a list of services (ports) that are inaccessible to computers on your LAN when service blocking is effective. To remove a service from this list, select the service, and click **Delete**.
Type	Select **TCP**, **UDP** or **TCP and UDP**, based on which one the custom port uses.
Port Number	Enter the range of port numbers that defines the service. For example, suppose you want to define the Gnutella service. Select **TCP** type and enter a port range of **6345-6349**.

Table 54 Security > Firewall

LABEL	DESCRIPTION
Add	Click this to add the selected service in **Available Services** to the **Blocked Services** list. Note that the service is blocked immediately after clicking this.
Delete	Select a service in the **Blocked Services**, and click this to remove the service from the list.
Clear All	Click this to remove all the services in the **Blocked Services** list.
Apply	Click this to enable LAN-to-WAN services blocking.
Reset	Click this to set every field in this screen to its last-saved value.

14.3 Firewall Technical Reference

This section provides some technical background information about the topics covered in this chapter.

14.3.1 Firewall Rules Overview

Your customized rules take precedence and override the ZyXEL Device's default settings. The ZyXEL Device checks the source IP address, destination IP address and IP protocol type of network traffic against the firewall rules (in the order you list them). When the traffic matches a rule, the ZyXEL Device takes the action specified in the rule.

14.3.2 Guidelines For Enhancing Security With Your Firewall

1. Change the default password via web configurator.
2. Think about access control before you connect to the network in any way.
3. Limit who can access your ZyXEL Device.
4. Don't enable any local service (such as telnet or FTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
5. For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
6. Keep the firewall in a secured (locked) room.

14.3.3 Security Considerations

Note: Incorrectly configuring the firewall may block valid access or introduce security risks to the ZyXEL Device and your protected network. Use caution when creating or deleting firewall rules and test your rules after you configure them.

Consider these security ramifications before creating a rule:

1. Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?

2. Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?

3. Does a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users may be able to connect to computers with running FTP servers.

4. Does this rule conflict with any existing rules?

Once these questions have been answered, adding rules is simply a matter of entering the information into the correct fields in the web configurator screens.

15

Certificates

15.1 Overview

The ZyXEL Device can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

15.1.1 What You Can Do in this Chapter

- Use the **My Certificate** screens (see Section 15.2 on page 212) to view and import the ZyXEL Device's CA-signed certificates.
- Use the **Trusted CA** screens (see Section 15.3 on page 214) to save the certificates of trusted CAs to the ZyXEL Device. You can also export the certificates to a computer.

15.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter.

Certification Authorities

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities.

Public and Private Keys

When using public-key cryptology for authentication, each host has two keys. One key is public and can be made openly available; the other key is private and must be kept secure. Public-key encryption in general works as follows.

1. Tim wants to send a private message to Jenny. Tim generates a public-private key pair. What is encrypted with one key can only be decrypted using the other.
2. Tim keeps the private key and makes the public key openly available.

3 Tim uses his private key to encrypt the message and sends it to Jenny.

4 Jenny receives the message and uses Tim's public key to decrypt it.

5 Additionally, Jenny uses her own private key to encrypt a message and Tim uses Jenny's public key to decrypt the message.

The ZyXEL Device uses certificates based on public-key cryptology to authenticate users attempting to establish a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

Certification Path

A certification path is the hierarchy of certification authority certificates that validate a certificate. The ZyXEL Device does not trust a certificate if any certificate on its path has expired or been revoked.

Certificate Directory Servers

Certification authorities maintain directory servers with databases of valid and revoked certificates. A directory of certificates that have been revoked before the scheduled expiration is called a CRL (Certificate Revocation List). The ZyXEL Device can check a peer's certificate against a directory server's list of revoked certificates. The framework of servers, software, procedures and policies that handles keys is called PKI (public-key infrastructure).

Advantages of Certificates

Certificates offer the following benefits.

- The ZyXEL Device only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

Certificate File Formats

The certification authority certificate that you want to import has to be in one of these file formats:

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses 64 ASCII characters to convert a binary X.509 certificate into a printable form.
- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. The ZyXEL Device currently allows the importation of a PKS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses 64 ASCII characters to convert a binary PKCS#7 certificate into a printable form.

Note: Be careful not to convert a binary file to text during the transfer process. It is easy for this to occur since many programs use text files by default.

15.1.3 Verifying a Certificate

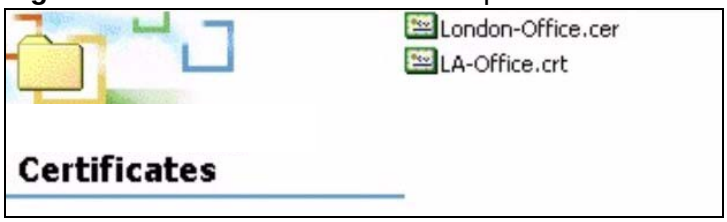
Before you import a trusted CA or trusted remote host certificate into the ZyXEL Device, you should verify that you have the actual certificate. This is especially true of trusted CA certificates since the ZyXEL Device also trusts any valid certificate signed by any of the imported trusted CA certificates.

You can use a certificate's fingerprint to verify it. A certificate's fingerprint is a message digest calculated using the MD5 or SHA1 algorithms. The following procedure describes how to check a certificate's fingerprint to verify that you have the actual certificate.

1 Browse to where you have the certificate saved on your computer.

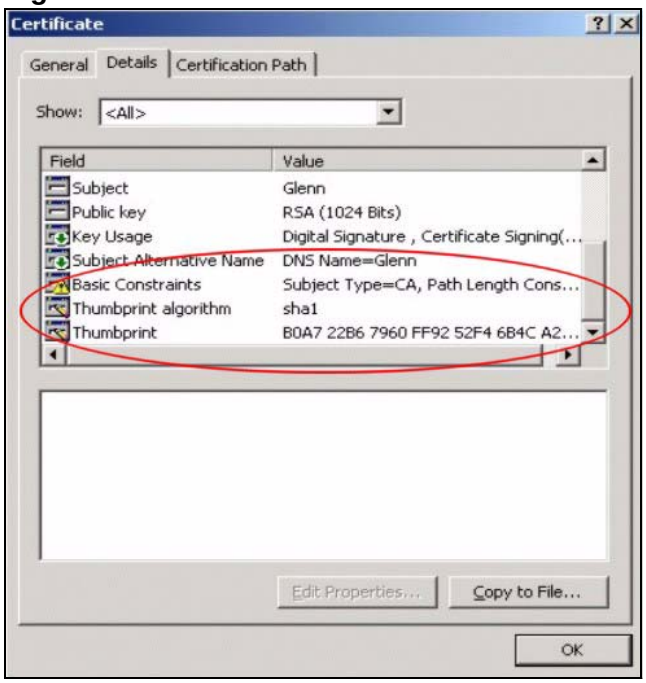
2 Make sure that the certificate has a ".cer" or ".crt" file name extension.

Figure 71 Certificates on Your Computer



3 Double-click the certificate's icon to open the **Certificate** window. Click the **Details** tab and scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.

Figure 72 Certificate Details



4 Use a secure method to verify that the certificate owner has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields. The secure method may very based on your situation. Possible examples would be over the telephone or through an HTTPS connection.

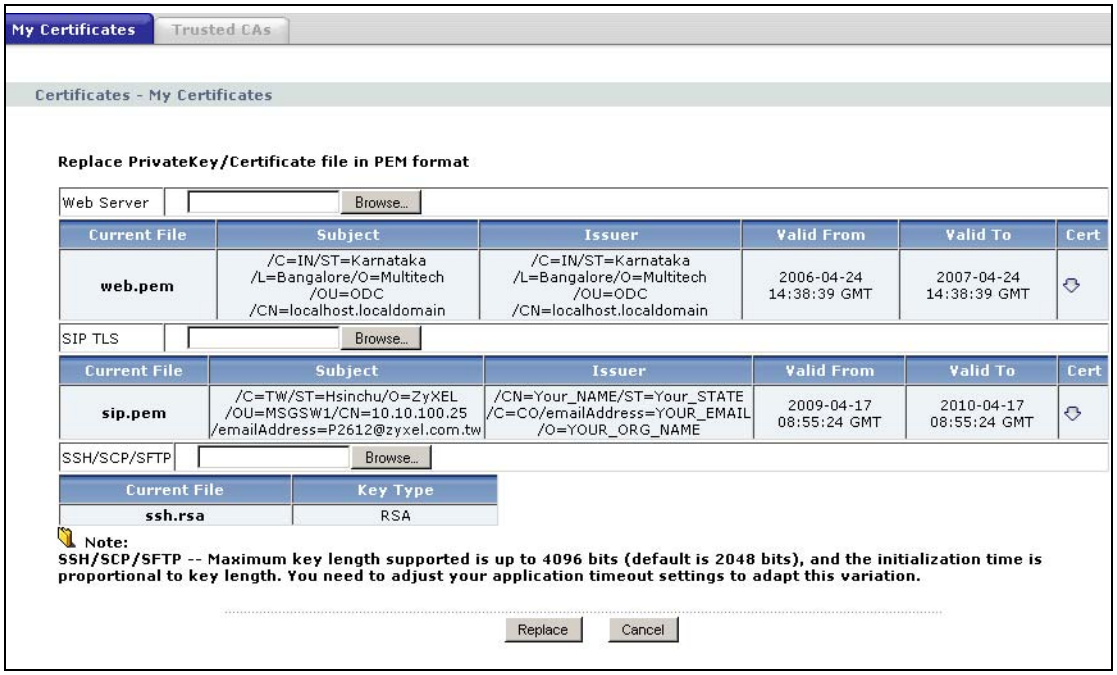
15.2 My Certificates

Use this screen to view the ZyXEL Device's summary list of certificates and certification requests. You can import the following certificates to your ZyXEL Device:

- Web Server - This certificate secures HTTP connections.
- SIP TLS - This certificate secures VoIP connections.
- SSH/SCP/SFTP - This certificate secures remote connections.

Click **Security > Certificates > My Certificates** to open the **My Certificates** screen.

Figure 73 Security > Certificates > My Certificates



The following table describes the labels in this screen.

Table 55 Security > Certificates > My Certificates

LABEL	DESCRIPTION
Web Server/ SIP TLS/ SSH/ SCP/SFTP	Type in the location of the file you want to upload in this field or click **Browse** to find it.
Browse	Click **Browse** to find the certificate file you want to upload.
Current File	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Subject	This field displays identifying information about the certificate's owner, such as **CN** (Common Name), **OU** (Organizational Unit or department), **O** (Organization or company) and **C** (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a **Not Yet Valid!** message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an **Expiring!** or **Expired!** message if the certificate is about to expire or has already expired.

Table 55 Security > Certificates > My Certificates (continued)

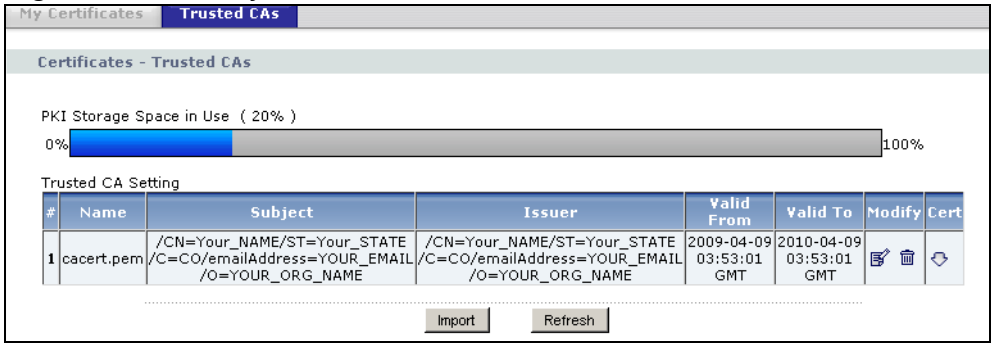
LABEL	DESCRIPTION
Cert	Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
Key Type	This field applies to the **SSH / SCP / SFTP** certificate. This shows the file format of the current certificate.
Replace	Click this to replace the certificate(s) and save your changes back to the ZyXEL Device.
Cancel	Click this to clear your settings.

15.3 Trusted CAs

Use this screen to view a summary list of certificates of the certification authorities that you have set the ZyXEL Device to accept as trusted. The ZyXEL Device accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities.

Click **Security > Certificates > Trusted CAs** to open the **Trusted CAs** screen.

Figure 74 Security > Certificates > Trusted CAs


My Certificates
Trusted CAs
Certificates - Trusted CAs
PKI Storage Space in Use (20%)
0%
100%
Trusted CA Setting
Name Subject Issuer Valid From Valid To Modify Cert
1 cacert.pem /CN=Your_NAME/ST=Your_STATE /C=CO/emailAddress=YOUR_EMAIL /O=YOUR_ORG_NAME /CN=Your_NAME/ST=Your_STATE /C=CO/emailAddress=YOUR_EMAIL /O=YOUR_ORG_NAME 2009-04-09 03:53:01 GMT 2010-04-09 03:53:01 GMT
Import
Refresh

The following table describes the labels in this screen.

Table 56 Security > Certificates > Trusted CAs

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyXEL Device's PKI storage space that is currently in use. The bar turns from blue to red when the maximum is being approached. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.
Trusted CA Setting	
#	This field displays the certificate index number. The certificates are listed in alphabetical order.

Table 56 Security > Certificates > Trusted CAs (continued)

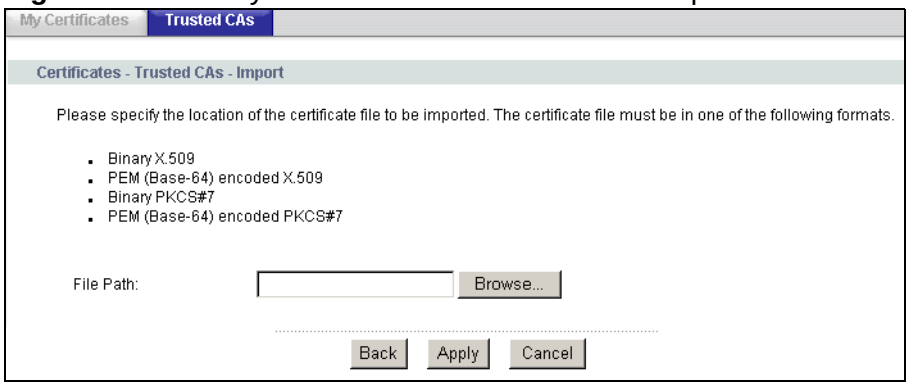
LABEL	DESCRIPTION
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a **Not Yet Valid!** message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an **Expiring!** or **Expired!** message if the certificate is about to expire or has already expired.
Modify	Click the **Edit** icon to open a screen with an in-depth list of information about the certificate. Click the **Remove** icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificates. Note that subsequent certificates move up by one when you take this action.
Cert	Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
Import	Click **Import** to open a screen where you can save the certificate of a certification authority that you trust, from your computer to the ZyXEL Device.
Refresh	Click this button to display the current validity status of the certificates.

15.4 Trusted CA Import

Click **Security** > **Certificates** > **Trusted CAs** to open the **Trusted CAs** screen and then click **Import** to open the **Trusted CA Import** screen. Follow the instructions in this screen to save a trusted certification authority's certificate to the ZyXEL Device.

Note: You must remove any spaces from the certificate's filename before you can import the certificate.

Figure 75 Security > Certificates > Trusted CA > Import



The following table describes the labels in this screen.

Table 57 Security > Certificates > Trusted CA > Import

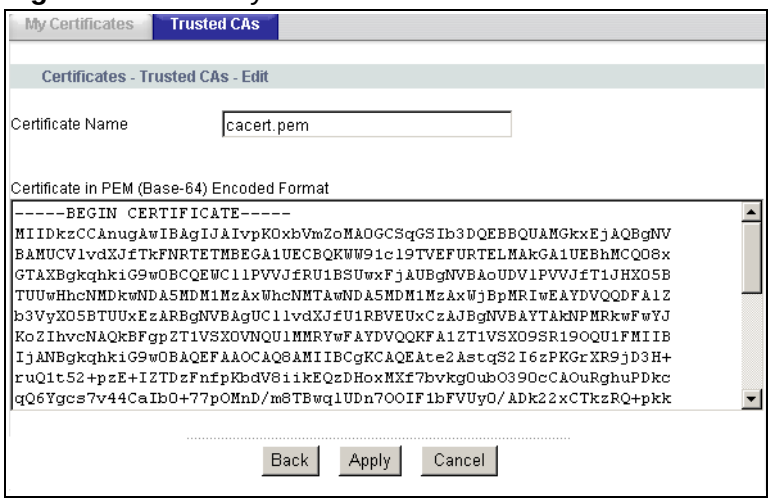
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it.
Browse	Click **Browse** to find the certificate file you want to upload.
Back	Click **Back** to return to the previous screen.
Apply	Click this to save the certificate on the ZyXEL Device.
Cancel	Click this to quit and return to the **Trusted CAs** screen.

15.5 Trusted CA Details

Use this screen to view in-depth information about the certification authority's certificate, change the certificate's name and set whether or not you want the ZyXEL Device to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority.

Click **Security** > **Certificates** > **Trusted CAs** to open the **Trusted CAs** screen. Click the details icon to open the **Trusted CA Details** screen.

Figure 76 Security > Certificates > Trusted CA > Details



The following table describes the labels in this screen.

Table 58 Security > Certificates > Trusted CA > Details

LABEL	DESCRIPTION
Certificate Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You may use any character (not including spaces).
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Back	Click this to return to the previous screen.
Apply	Click this to save your changes back to the ZyXEL Device. You can only change the name and/or set whether or not you want the ZyXEL Device to check the CRL that the certification authority issues before trusting a certificate issued by the certification authority.
Cancel	Click this to quit and return to the **Trusted CAs** screen.

16

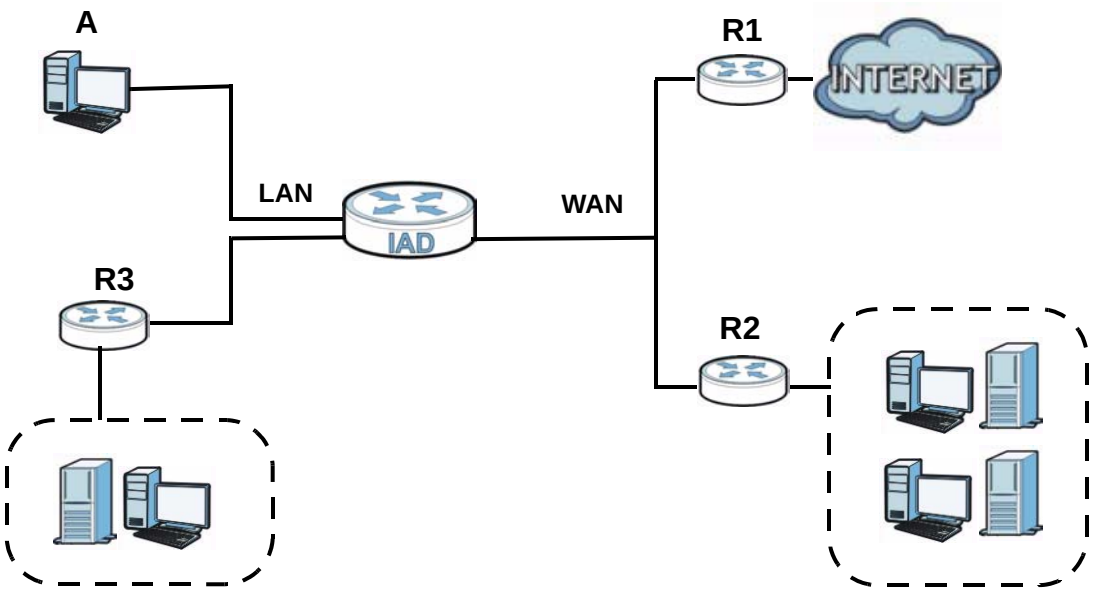
Static Route

16.1 Overview

The ZyXEL Device usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the ZyXEL Device send data to devices not reachable through the default gateway, use static routes.

For example, the next figure shows a computer (**A**) connected to the ZyXEL Device's LAN interface. The ZyXEL Device routes most traffic from **A** to the Internet through the ZyXEL Device's default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**. You create another static route to communicate with a separate network behind a router **R3** connected to the LAN.

Figure 77 Example of Static Routing Topology



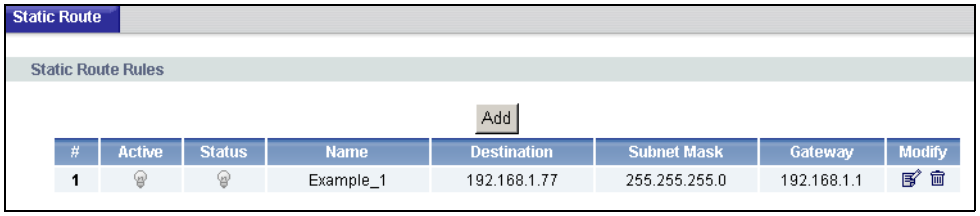
16.1.1 What You Can Do in this Chapter

Use the **Static Route** screens (Section 16.2 on page 220) to view and configure IP static routes on the ZyXEL Device.

16.2 Configuring Static Route

Use this screen to view and configure IP static routes on the ZyXEL Device. Click **Advanced > Static Route** to open the **Static Route** screen.

Figure 78 Advanced > Static Route


Static Route
Static Route Rules
Add
Active Status Name Destination Subnet Mask Gateway Modify
1 Example_1 192.168.1.77 255.255.255.0 192.168.1.1

The following table describes the labels in this screen.

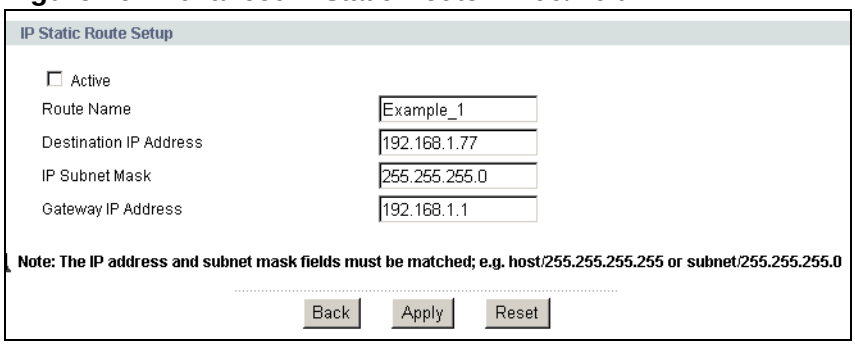
Table 59 Advanced > Static Route

LABEL	DESCRIPTION
Add	Click this to go to the screen where you can set up a static route on the ZyXEL Device.
#	This is the number of an individual static route.
Active	This indicates whether the rule is active or not. You can change this in the **Modify** screen (Section 16.2.1 on page 221).
Status	This shows whether the rule is currently in use or not.
Name	This is the name that describes or identifies this route.
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Subnet Mask	This parameter specifies the IP network subnet mask of the final destination.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Modify	Click the **Edit** icon to go to the screen where you can set up a static route on the ZyXEL Device. Click the **Remove** icon to remove a static route from the ZyXEL Device. A window displays asking you to confirm that you want to delete the route.

16.2.1 Static Route Add/Edit

Select a static route index number and click **Add** or **Edit**. The screen shown next appears. Use this screen to configure the required information for a static route.

Figure 79 Advanced > Static Route > Add/Edit



The following table describes the labels in this screen.

Table 60 Advanced > Static Route > Add/Edit

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this static route.
Route Name	Enter the name of the IP static route. Leave this field blank to delete this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway IP Address	Enter the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to begin configuring this screen afresh.

17

Quality of Service (QoS)

17.1 Overview

This chapter discusses the ZyXEL Device's **QoS** screens. Use these screens to set up your ZyXEL Device to use QoS for traffic management.

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. QoS allows the ZyXEL Device to group and prioritize application traffic and fine-tune network performance.

Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

The ZyXEL Device assigns each packet a priority and then queues the packet accordingly. Packets assigned a high priority are processed more quickly than those with low priority if there is congestion, allowing time-sensitive applications to flow more smoothly. Time-sensitive applications include both those that require a low level of latency (delay) and a low level of jitter (variations in delay) such as Internet gaming, and those for which jitter alone is a problem such as Internet radio or streaming video.

Note: The ZyXEL Device has built-in configurations for Voice over IP (IP). The Quality of Service (QoS) feature does not affect VoIP traffic.

- See Section 17.6 on page 233 for advanced technical information on SIP.

17.1.1 What You Can Do in this Chapter

- Use the **General** screen (Section 17.2 on page 224) to enable QoS on the ZyXEL Device and decide allowable bandwidth using QoS.
- Use the **Queue Setup** screen (Section 17.3 on page 226) lets you configure QoS queue assignment.
- Use the **Class Setup** screen (Section 17.4 on page 227) to set up classifiers to sort traffic into different flows and assign priority and define actions to be performed for a classified traffic flow.

- Use the **Monitor** screen (Section 17.5 on page 233) to view the ZyXEL Device's QoS-related packet statistics.

17.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter.

QoS versus Cos

QoS is used to prioritize source-to-destination traffic flows. All packets in the same flow are given the same priority. CoS (class of service) is a way of managing traffic in a network by grouping similar types of traffic together and treating each type as a class. You can use CoS to give different priorities to different packet types.

CoS technologies include IEEE 802.1p layer 2 tagging and DiffServ (Differentiated Services or DS). IEEE 802.1p tagging makes use of three bits in the packet header, while DiffServ is a new protocol and defines a new DS field, which replaces the eight-bit ToS (Type of Service) field in the IP header.

Tagging and Marking

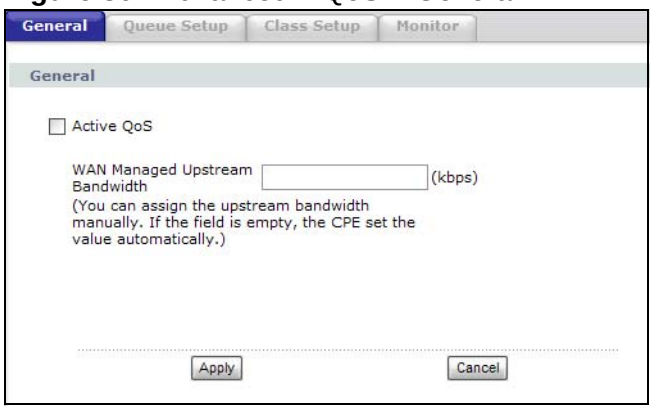
In a QoS class, you can configure whether to add or change the DSCP (DiffServ Code Point) value, IEEE 802.1p priority level and VLAN ID number in a matched packet. When the packet passes through a compatible network, the networking device, such as a backbone switch, can provide specific treatment or service based on the tag or marker.

17.2 The QoS General Screen

Use this screen to enable or disable QoS, and select to have the ZyXEL Device assign the allowable upstream bandwidth.

Click **Advanced > QoS > General** to open the screen as shown next.

Figure 80 Advanced > QoS > General



The following table describes the labels in this screen.

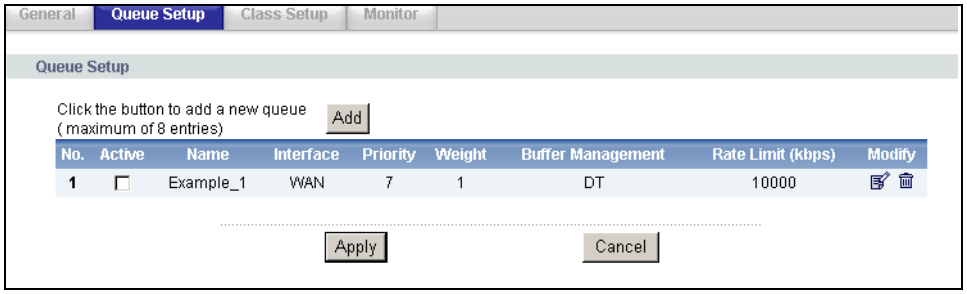
Table 61 Advanced > QoS > General

LABEL	DESCRIPTION
Active QoS	Select the check box to turn on QoS to improve your network performance. You can give priority to traffic that the ZyXEL Device forwards out through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.
WAN Managed Upstream Bandwidth	Enter the amount of bandwidth for the WAN interface that you want to allocate using QoS. The recommendation is to set this speed to match the interface's actual transmission speed. For example, set the WAN interface speed to 100000 kbps if your Internet connection has an upstream transmission speed of 100 Mbps. Setting this number higher than the interface's actual transmission speed will stop lower priority traffic from being sent if higher priority traffic uses all of the actual bandwidth. If you set this number lower than the interface's actual transmission speed, the ZyXEL Device will not use some of the interface's available bandwidth. Leave this field blank to have the ZyXEL Device set this value automatically.
Apply	Click this to save your settings back to the ZyXEL Device.
Cancel	Click this to begin configuring this screen afresh.

17.3 The Queue Setup Screen

Use this screen to configure QoS queue assignment. Click **QoS > Queue Setup** to open the screen as shown next.

Figure 81 Advanced > QoS > Queue Setup



The following table describes the labels in this screen.

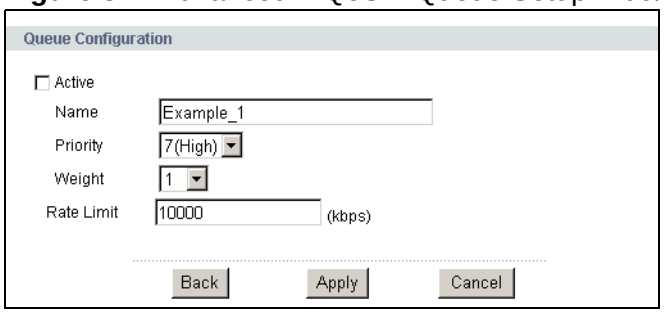
Table 62 Advanced > QoS > Queue Setup

LABEL	DESCRIPTION
Add	Click this button to create a new entry.
No.	This is the index number of this entry.
Active	Select the check box to enable the queue.
Name	This shows the descriptive name of this queue.
Interface	This shows the name of the ZyXEL Device's interface through which traffic in this queue passes.
Priority	This shows the priority of this queue.
Weight	This shows the weight of this queue.
Buffer Management	This shows the queue management algorithm used by the ZyXEL Device.
Rate Limit (kbps)	This shows the maximum transmission rate allowed for traffic on this queue.
Modify	Click the **Edit** icon to go to the screen where you can edit the queue. Click the **Remove** icon to delete an existing queue. Note that subsequent rules move up by one when you take this action.
Apply	Click this to save your changes back to the ZyXEL Device.
Cancel	Click this to begin configuring this screen afresh.

17.3.1 Adding/Editing a QoS Queue

Use this screen to configure a queue. Click the **Add** button or the edit icon in the **Queue Setup** screen.

Figure 82 Advanced > QoS > Queue Setup: Add/Edit



The following table describes the labels in this screen.

Table 63 Advanced > QoS > Queue Setup: Add/Edit

LABEL	DESCRIPTION
Active	Select to enable or disable this queue.
Name	Enter the descriptive name of this queue.
Priority	Select the priority level (from 1 to 7) of this queue. The smaller the number, the higher the priority level. Traffic assigned to higher priority queues gets through faster while traffic in lower priority queues is dropped if the network is congested.
Weight	Select the weight (from 1 to 15) of this queue. If two queues have the same priority level, the ZyXEL Device divides the bandwidth across the queues according to their weights. Queues with larger weights get more bandwidth than queues with smaller weights.
Rate Limit	Specify the maximum transmission rate (in Kbps) allowed for traffic on this queue.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes back to the ZyXEL Device.
Cancel	Click this to begin configuring this screen afresh.

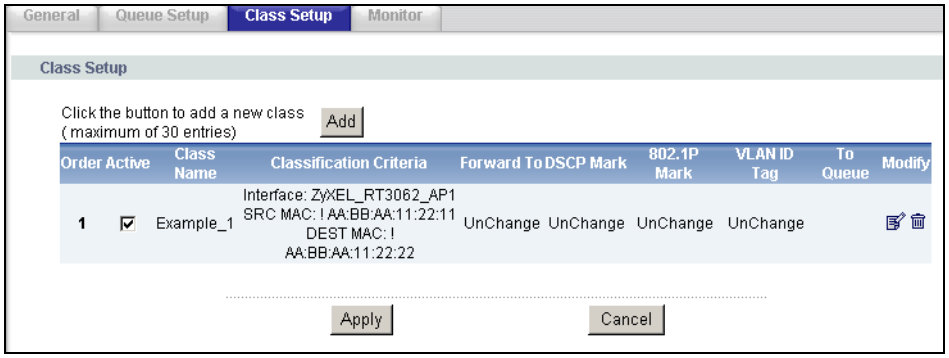
17.4 The Class Setup Screen

Use this screen to add, edit or delete QoS classifiers. A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming interface. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow.

You can give different priorities to traffic that the ZyXEL Device forwards out through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.

Click **Advanced > QoS > Class Setup** to open the following screen.

Figure 83 Advanced > QoS > Class Setup



The following table describes the labels in this screen.

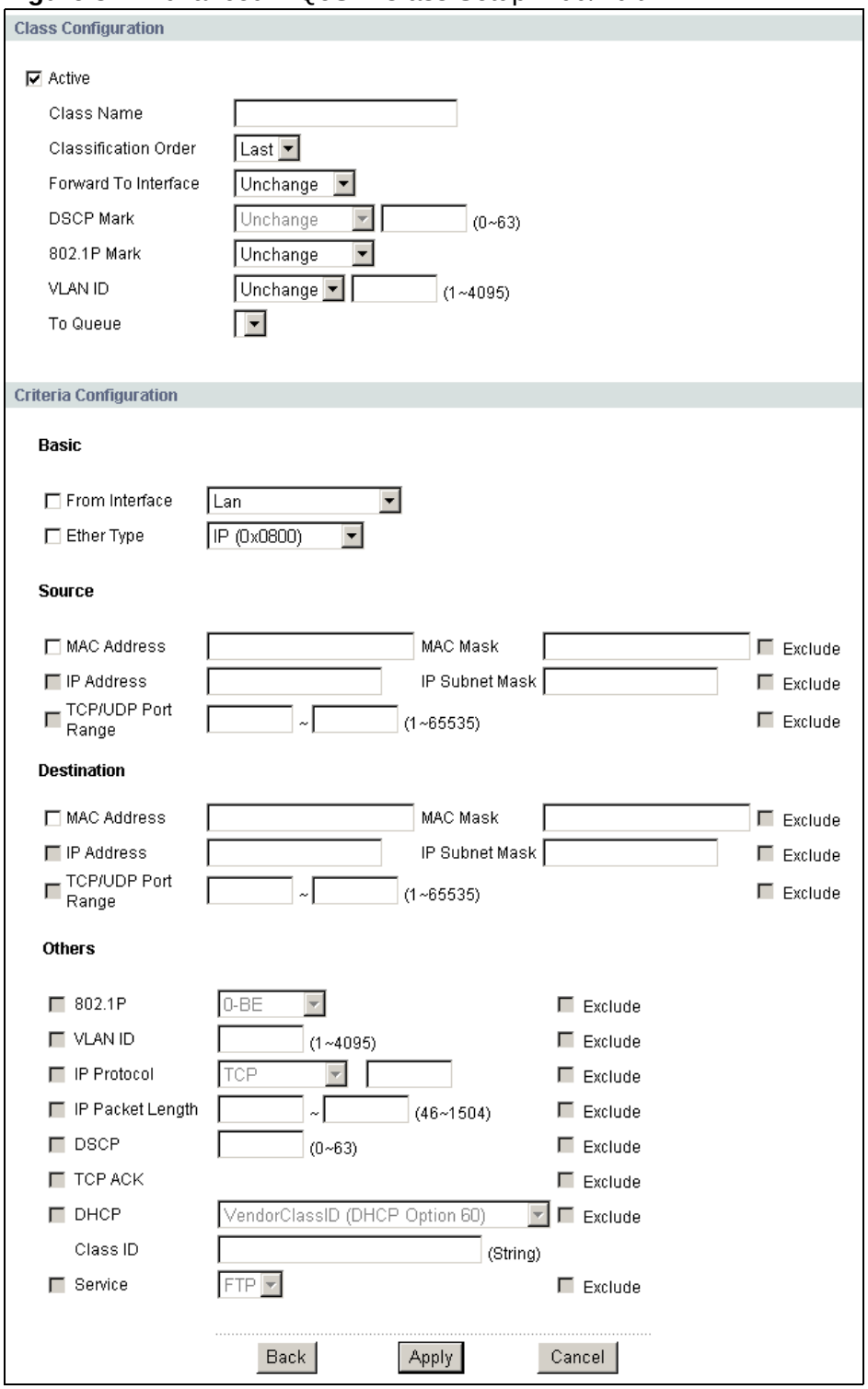
Table 64 Advanced > QoS > Class Setup

LABEL	DESCRIPTION
Add	Click this button to create a new classifier.
Order	This field displays the order number of the classifier.
Active	Select the check box to enable the classifier.
Class Name	This is the name of the classifier.
Classification Criteria	This shows criteria specified in this classifier, for example the interface from which traffic of this class should come and the source MAC address of traffic that matches this classifier.
Forward To	This is the interface through which traffic that matches this classifier is forwarded out.
DSCP Mark	This is the DSCP number added to traffic of this classifier.
802.1P Mark	This is the IEEE 802.1p priority level assigned to traffic of this classifier.
VLAN ID Tag	This is the VLAN ID number assigned to traffic of this classifier.
To Queue	This is the name of the queue in which traffic of this classifier is put.
Modify	Click the **Edit** icon to go to the screen where you can edit the classifier. Click the **Remove** icon to delete an existing classifier. Note that subsequent rules move up by one when you take this action.
Apply	Click this to save your changes back to the ZyXEL Device.
Cancel	Click this to begin configuring this screen afresh.

17.4.1 QoS Class Add/Edit

Click the **Add** button or the **Edit** icon in the **Class Setup** screen to configure a classifier.

Figure 84 Advanced > QoS > Class Setup: Add/Edit



The following table describes the labels in this screen.

Table 65 Advanced > QoS > Class Setup: Add/Edit

LABEL	DESCRIPTION
Class Configuration	
Active	Select to enable or disable this classifier.
Class Name	Enter a descriptive name of up to 32 printable English keyboard characters, including spaces.
Classification Order	Select an existing number for where you want to put this classifier to move the classifier to the number you selected after clicking **Apply**. Select **Last** to put this rule in the back of the classifier list.
Forward to Interface	Select a WAN interface through which traffic of this class will be forwarded out. If you select **Unchange**, the ZyXEL Device forward traffic of this class according to the default routing table.
DSCP Mark	This field is available only when you select the **Ether Type** check box. If you select **Mark**, enter a DSCP value with which the ZyXEL Device replaces the DSCP field in the packets. If you select **Auto Mapping** and there is a VLAN tag carried in the matched packets, the ZyXEL Device will replace the IP ToS field with the 802.1p priority field. If you select **Unchange**, the ZyXEL Device keep the DSCP field in the packets.
802.1p Mark	Select a priority level with which the ZyXEL Device replaces the IEEE 802.1p priority field in the packets. If you select **Unchange**, the ZyXEL Device keep the 802.1p priority field in the packets.
VLAN ID	If you select **Remark**, enter a VLAN ID number (between 1 and 4095) with which the ZyXEL Device replaces the VLAN ID of the frames. If you select **Remove**, the ZyXEL Device deletes the VLAN ID of the frames before forwarding them out. If you select **Add**, the ZyXEL Device treat all matched traffic untagged and add a second VLAN ID. If you select **Unchange**, the ZyXEL Device keep the VLAN ID in the packets.
To Queue	Select a queue that applies to this class. You should have configured a queue in the **Queue Setup** screen already.
Criteria Configuration Use the following fields to configure the criteria for traffic classification.	
Basic	
From Interface	Select whether the traffic class comes from the LAN or a wireless interface.

Table 65 Advanced > QoS > Class Setup: Add/Edit

LABEL	DESCRIPTION
Ether Type	Select a predefined application to configure a class for the matched traffic. If you select **IP**, you also need to configure source or destination MAC address, IP address, DHCP options, DSCP value or the protocol type. If you select **8021Q**, you can configure an 802.1p priority level and VLAN ID in the **Others** section.
Source	
MAC Address	Select the check box and enter the source MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
IP Address	Select the check box and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
IP Subnet Mask	Enter the source subnet mask.
TCP/UDP Port Range	If you select **TCP** or **UDP** in the **IP Protocol** field, select the check box and enter the port number(s) of the source.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Destination	
MAC Address	Select the check box and enter the destination MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
IP Address	Select the check box and enter the destination IP address in dotted decimal notation. A blank source IP address means any source IP address.
IP Subnet Mask	Enter the destination subnet mask.
TCP/UDP Port Range	If you select **TCP** or **UDP** in the **IP Protocol** field, select the check box and enter the port number(s) of the source.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Others	

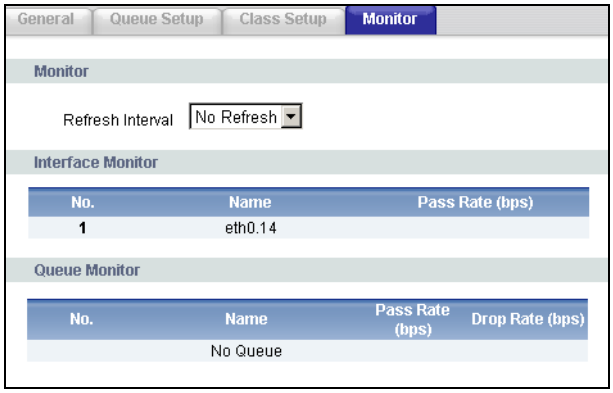
Table 65 Advanced > QoS > Class Setup: Add/Edit

LABEL	DESCRIPTION
802.1P	This field is available only when you select **802.1Q** in the **Ether Type** field. Select this option and select a priority level (between 0 and 7) from the drop down list box. "0" is the lowest priority level and "7" is the highest.
VLAN ID	This field is available only when you select **802.1Q** in the **Ether Type** field. Select this option and specify a VLAN ID number between 1 and 4095.
IP Protocol	This field is available only when you select **IP** in the **Ether Type** field. Select this option and select the protocol (service type) from **TCP** or **UDP**. If you select **User defined**, enter the protocol (service type) number.
IP Packet Length	This field is available only when you select **IP** in the **Ether Type** field. Select this option and enter the minimum and maximum packet length (from 46 to 1504) in the fields provided.
DSCP	This field is available only when you select **IP** in the **Ether Type** field. Select this option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.
TCP ACK	This field is available only when you select **IP** in the **Ether Type** field. If you select this option, the matched TCP packets must contain the ACK (Acknowledge) flag.
DHCP	This field is available only when you select **IP** in the **Ether Type** field, and **UDP** in the **IP Protocol** field. Select this option and select a DHCP option. If you select **Vendor Class ID (DHCP Option 60)**, enter the **Class ID** of the matched traffic, such as the type of the hardware or firmware. If you select **ClientID (DHCP Option 61)**, enter the **Type** of the matched traffic and **Client ID** of the DHCP client. If you select **User Class ID (DHCP Option 77)**, enter the **User Class Data**, which is a string that identifies the user's category or application type in the matched DHCP packets. If you select **VendorSpecificIntro (DHCP Option 125)**, enter the **Enterprise Number** of the software of the matched traffic and **Vendor Class Data** used by all the DHCP clients.
Service	Select the service classification of the traffic.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Back	Click this to return to the previous screen without saving.
Apply	Click this to save your changes back to the ZyXEL Device.
Cancel	Click this to begin configuring this screen afresh.

17.5 The QoS Monitor Screen

To view the ZyXEL Device's QoS packet statistics, click **Advanced > QoS > Monitor**. The screen appears as shown.

Figure 85 Advanced > QoS > Monitor



The following table describes the labels in this screen.

Table 66 Advanced > QoS > Monitor

LABEL	DESCRIPTION
Refresh Interval	Enter how often you want the ZyXEL Device to update this screen. Select **No Refresh** to stop refreshing statistics.
Interface Monitor	
No.	This is the index number of the entry.
Name	This shows the name of the WAN interface on the ZyXEL Device.
Pass Rate (bps)	This shows how many packets forwarded to this interface are transmitted successfully.
Queue Monitor	
No.	This is the index number of the entry.
Name	This shows the name of the queue.
Pass Rate (bps)	This shows how many packets assigned to this queue are transmitted successfully.
Drop Rate (bps)	This shows how many packets assigned to this queue are dropped.

17.6 QoS Technical Reference

This section provides some technical background information about the topics covered in this chapter.

17.6.1 IEEE 802.1Q Tag

The IEEE 802.1Q standard defines an explicit VLAN tag in the MAC header to identify the VLAN membership of a frame across bridges. A VLAN tag includes the 12-bit VLAN ID and 3-bit user priority. The VLAN ID associates a frame with a specific VLAN and provides the information that devices need to process the frame across the network.

IEEE 802.1p specifies the user priority field and defines up to eight separate traffic types. The following table describes the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).

Table 67 IEEE 802.1p Priority Level and Traffic Type

PRIORITY LEVEL	TRAFFIC TYPE
Level 7	Typically used for network control traffic such as router configuration messages.
Level 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
Level 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.
Level 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.
Level 3	Typically used for “excellent effort” or better than best effort and would include important business traffic that can tolerate some delay.
Level 2	This is for “spare bandwidth”.
Level 1	This is typically used for non-critical “background” traffic such as bulk transfers that are allowed but that should not affect other applications and users.
Level 0	Typically used for best-effort traffic.

17.6.2 IP Precedence

Similar to IEEE 802.1p prioritization at layer-2, you can use IP precedence to prioritize packets in a layer-3 network. IP precedence uses three bits of the eight-bit ToS (Type of Service) field in the IP header. There are eight classes of services (ranging from zero to seven) in IP precedence. Zero is the lowest priority level and seven is the highest.

17.6.3 DiffServ

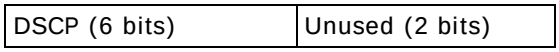
QoS is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

DiffServ (Differentiated Services) is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.



The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different kinds of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

18

Dynamic DNS Setup

18.1 Overview

This chapter discusses how to configure your ZyXEL Device to use Dynamic DNS.

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in applications such as NetMeeting and CU-SeeMe). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

18.1.1 What You Can Do in the DDNS Screen

Use the **Dynamic DNS** screen (Section 18.2 on page 238) to enable DDNS and configure the DDNS settings on the ZyXEL Device.

18.1.2 What You Need To Know About DDNS

DYNDNS Wildcard

Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

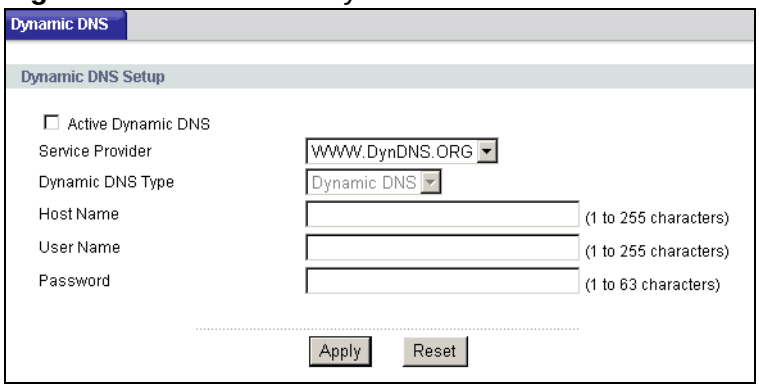
If you have a private WAN IP address, then you cannot use Dynamic DNS.

18.2 Configuring Dynamic DNS

To change your ZyXEL Device's DDNS, click **Advanced > Dynamic DNS**. The screen appears as shown.

See Section 18.1 on page 237 for more information.

Figure 86 Advanced > Dynamic DNS



The following table describes the fields in this screen.

Table 68 Advanced > Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS Setup	
Active Dynamic DNS	Select this check box to use dynamic DNS.
Service Provider	This is the name of your Dynamic DNS service provider.
Dynamic DNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider.
Host Name	Type the domain name assigned to your ZyXEL Device by your Dynamic DNS provider. You can specify up to two host names in the field separated by a comma (",").
User Name	Type your user name.
Password	Type the password assigned to you.
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to begin configuring this screen afresh.

19

Service Control

19.1 Overview

This chapter provides information on the Service Control screens.

Service Control allows you to manage your ZyXEL Device from a remote location through the following interfaces:

- LAN and WLAN
- WAN only

Note: The ZyXEL Device is managed using the Web Configurator.

19.1.1 What You Can Do in this Chapter

Use the **Service Control** screens (Section 19.2 on page 240) to configure through which interface(s) users can use which service(s) to manage the ZyXEL Device.

19.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter

TR-064

TR-064 is a LAN-Side DSL CPE Configuration protocol defined by the DSL Forum. TR-064 is built on top of UPnP. It allows the users to use a TR-064 compliant CPE management application on their computers from the LAN to discover the CPE and configure user-specific parameters, such as the username and password.

SSH/SCP/SFTP

Secure Shell (SSH) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network. The following file transfer methods use SSH:

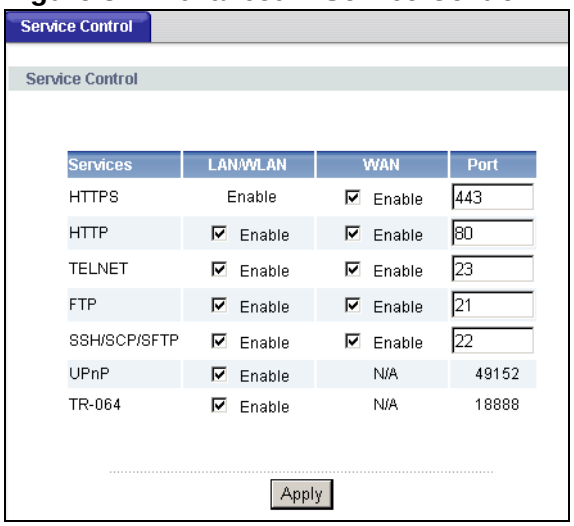
- **Secure Copy (SC)** is a secure way of transferring files between computers. It uses port 22.
- **SSH File Transfer Protocol or Secure File Transfer Protocol (SFTP)** is an old way of transferring files between computers. It uses port 22.

19.2 The Service Control Screen

Use this screen to decide what services you may use to access which ZyXEL Device interface.

Click **Advanced > Service Control** to open the following screen.

Figure 87 Advanced > Service Control



The following table describes the fields in this screen.

Table 69 Advanced > Service Control

LABEL	DESCRIPTION
#	This is the index number of the entry.
Services	This is the service you may use to access the ZyXEL Device.
LAN/WLAN	Select the **Enable** check box for the corresponding services that you want to allow access to the ZyXEL Device from the LAN and WLAN.
WAN	Select the **Enable** check box for the corresponding services that you want to allow access to the ZyXEL Device from the WAN.
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Apply	Click this button to save your changes back to the ZyXEL Device.

PART III
Maintenance, Troubleshooting and Specifications

System (243)

Logs (247)

Tools (253)

Diagnostic (265)

Account (269)

Troubleshooting (271)

Product Specifications (279)

20 System

20.1 Overview

This chapter shows you how to configure system related settings, such as system time, password, name, the domain name and the inactivity timeout interval.

20.1.1 What You Can Do in this Chapter

- Use the **General** screen (Section 20.2 on page 244) to configure system settings.
- Use the **Time Setting** screen (Section 20.3 on page 245) to set the system time.

20.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter.

Domain Name

This is a network address that identifies the owner of a network connection. For example, in the network address “www.zyxel.com/support/files”, the domain name is “www.zyxel.com”.

DHCP

DHCP (Dynamic Host Configuration Protocol) is a method of allocating IP addresses to devices on a network from a DHCP Server. Often your ISP or a router on your network performs this function.

LAN

A LAN (local area network) is typically a network which covers a small area, made up of computers and other devices which share resources such as Internet access and printers.

20.2 The System General Screen

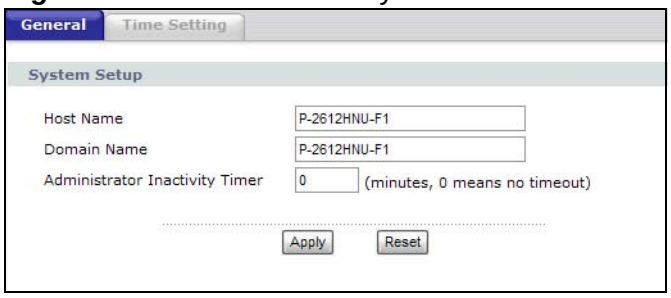
Use the **General** screen to configure system settings such as the system and domain name, inactivity timeout interval and system password.

The **Host Name** is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name". Find the system name of your Windows computer.

In Windows XP, click **start**, **My Computer**, **View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the ZyXEL Device **System Name**.

Click **Maintenance > System** to open the **General** screen.

Figure 88 Maintenance > System > General



The following table describes the labels in this screen.

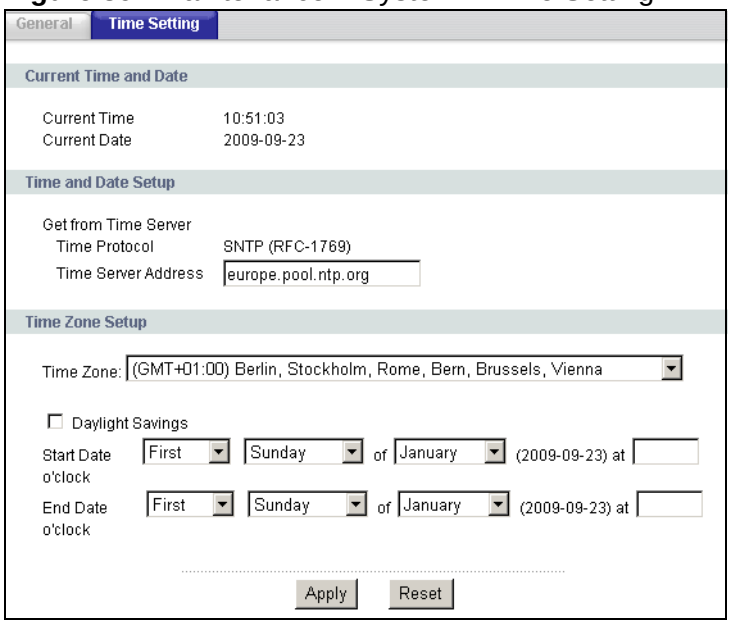
Table 70 Maintenance > System > General

LABEL	DESCRIPTION
General Setup	
Host Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. The domain name entered by you is given priority over the ISP assigned domain name.
Administrator Inactivity Timer	Type how many minutes a management session (either via the web configurator) can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to begin configuring this screen afresh.

20.3 The Time Setting Screen

To change your ZyXEL Device's time and date, click **Maintenance > System > Time Setting**. The screen appears as shown. Use this screen to configure the ZyXEL Device's time based on your local time zone.

Figure 89 Maintenance > System > Time Setting



The following table describes the fields in this screen.

Table 71 Maintenance > System > Time Setting

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the time of your ZyXEL Device.
Current Date	This field displays the date of your ZyXEL Device.
Time and Date Setup	
Get from Time Server	Select this radio button to have the ZyXEL Device get the time and date from the time server you specified below.
Time Protocol	This shows the time service protocol that your time server sends when you turn on the ZyXEL Device.
Time Server Address	Enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).

Table 71 Maintenance > System > Time Setting (continued)

LABEL	DESCRIPTION
Daylight Savings	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Daylight Savings**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Second**, **Sunday**, **March** and type 2 in the **o'clock** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Daylight Savings**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **November** and type 2 in the **o'clock** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click this to save your changes back to the ZyXEL Device.
Reset	Click this to begin configuring this screen afresh.

21 Logs

21.1 Overview

The web configurator allows you to choose which categories of events and/or alerts to have the ZyXEL Device log and then display the logs or have the ZyXEL Device send them to an administrator (as e-mail) or to a syslog server.

Note: The ZyXEL Device's log feature is only for Voice over IP (VoIP).

21.1.1 What You Can Do in this Chapter

- Use the **View Log** screen (Section 21.2 on page 248) to see the logs for the categories that you selected in the **Log Settings** screen.
- Use The **Log Settings** screen (Section 21.3 on page 249) to configure where the ZyXEL Device sends logs and which logs and/or immediate alerts the ZyXEL Device records.

21.1.2 What You Need To Know

The following terms and concepts may help as you read this chapter.

Alerts and Logs

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

Syslog Overview

The syslog protocol allows devices to send event notification messages across an IP network to syslog servers that collect the event messages. A syslog-enabled device can generate a syslog message and send it to a syslog server.

Syslog is defined in RFC 3164. The RFC defines the packet format, content and system log related information of syslog messages. Each syslog message has a

facility and severity level. The syslog facility identifies a file in the syslog server. Refer to the documentation of your syslog program for details. The following table describes the syslog severity levels.

Table 72 Syslog Severity Levels

CODE	SEVERITY
0	Emergency: The system is unusable.
1	Alert: Action must be taken immediately.
2	Critical: The system condition is critical.
3	Error: There is an error condition on the system.
4	Warning: There is a warning condition on the system.
5	Notice: There is a normal but significant condition on the system.
6	Informational: The syslog contains an informational message.
7	Debug: The message is intended for debug-level purposes.

21.2 The View Log Screen

Click **Maintenance > Logs** to open the **View Log** screen. Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see Section 21.3 on page 249).

Log entries in red indicate alerts. The log wraps around and deletes the old entries after it fills. Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.

Figure 90 Maintenance > Logs > View Log

The following table describes the fields in this screen.

Table 73 Maintenance > Logs > View Log

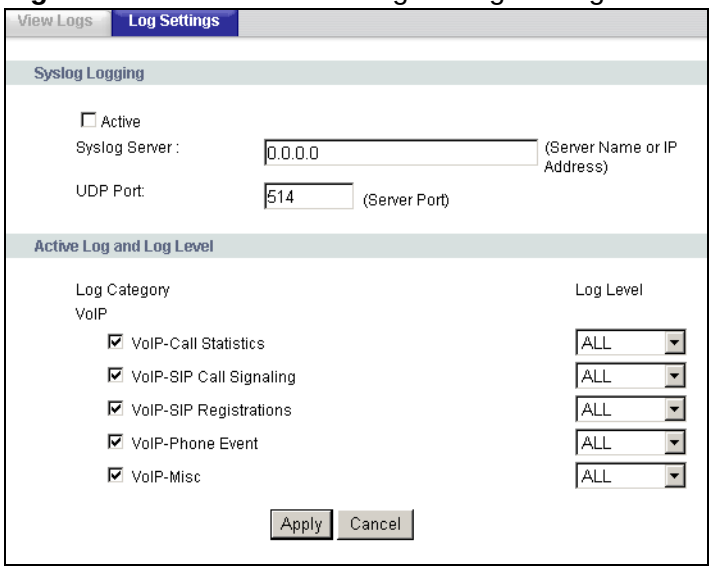
LABEL	DESCRIPTION
Display	The categories that you select in the **Log Settings** screen display in the drop-down list box. Select a category of logs to view; select **All Logs** to view logs from all of the log categories that you selected in the **Log Settings** page.
Level	Select the lowest severity level that you want to view.
Refresh	Click this to renew the log screen.
Clear Log	Click this to delete all the logs.
#	This field is a sequential value and is not associated with a specific entry.
Time	This field displays the time the log was recorded.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Level	This field displays the severity level of the logs that the device is to send to this syslog server.
Message	This field states the reason for the log.

21.3 The Log Settings Screen

Use the **Log Settings** screen to configure where the ZyXEL Device sends logs and which logs and/or immediate alerts the ZyXEL Device records.

To change your ZyXEL Device's log settings, click **Maintenance > Logs** > **Log Settings**. The screen appears as shown.

Figure 91 Maintenance > Logs > Log Settings



The following table describes the fields in this screen.

Table 74 Maintenance > Logs > Log Settings

LABEL	DESCRIPTION
Syslog Logging	The ZyXEL Device sends a log to an external syslog server.
Active	Click **Active** to enable syslog logging.
Syslog Server	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
UDP Port	Enter the port number used by the syslog server.
Active Log and Alert	
Log	Select the categories of logs that you want to record.
Send Immediate Alert	Select log categories for which you want the ZyXEL Device to send E-mail alerts immediately.
Apply	Click this to save your customized settings and exit this screen.
Cancel	Click this to return to the previously saved settings.

21.4 Log Descriptions

This section provides descriptions of example log messages.

Table 75 Call Statistics Logs

LOG MESSAGE	DESCRIPTION
`Start Outgoing Call [SIP Number]`	Someone used a phone to make an outgoing call.
`rx pkts %d,rx bytes %d,lost pkts %d,avg jitter %d,tx pkts %d,tx bytes %d`	Display the RTP packets status.
`In Call End [SIP Number],Duration: Seconds`	Incoming call from SIP number has terminated. Show the call duration.
`Out Call End [SIP Number],Duration: Seconds`	Outgoing call from SIP number has terminated. Show the call duration.
`Incoming Call Established [SIP Number]`	Incoming call from SIP number has been established.
`Outgoing Call Established [SIP Number]`	Outgoing call to SIP number has been established.

Table 76 SIP Call Signaling

LOG MESSAGE	DESCRIPTION
SIP Call Signaling [SIP number][port number] SIP Content - SIP Message Send	Send SIP message to SIP server.
SIP Call Signaling [SIP number][port number] SIP Content - SIP Message Received	Receive SIP message from SIP server.
SIP: Number DeRegister	The listed SIP account's registation was deleted from the SIP register server.
SIP: Number Register Success	The listed SIP account was successfully registered with from the SIP register server.

Table 77 Phone Event

LOG MESSAGE	DESCRIPTION
OFFHOOK	The phone is off the hook.
ONHOOK	The phone is on hook.
FLASH	The user pressed the flash key on phone.
Dtmf[%c]	The user pressed the digit number on phone.

Table 78 VoIP Miscellaneous

LOG MESSAGE	DESCRIPTION
Call return	User activated the phone feature; redialled the last incoming call.
temp. CLIP activated	Activate one-shot caller ID display.
temp. CLIR activated	Activate one-shot caller ID hidden.
Enable Call waiting	Activate call waiting.
Disable Call waiting	Deactivate call waiting.
Call transfer	Activate call transfer.
Enable CFU	Activate call forwarding unconditional to the registered destination.
Disable CFU	Deactivate call forwarding unconditional to the registered destination.
Enable CFNR	Activate call forwarding on No Reply to the registered destination.
Disable CFNR	DeActivate call forwarding on No Reply to the registered destination.
Enable CFB	Activate call forwarding on No Busy to the registered destination.

Table 78 VoIP Miscellaneous

LOG MESSAGE	DESCRIPTION
Disable CFB	DeActivate call forwarding on No Busy to the registered destination.
temp. enable CallWaiting	One-shot enable call waiting.
temp. disable CallWaiting	One-shot disable call waiting.
CallWaiting Interrogation	Interrogation the call waiting status.

22 Tools

22.1 Overview

Use the instructions in this chapter to change the device's configuration file or upgrade its firmware. After you configure your device, you can backup the configuration file to a computer. That way if you later misconfigure the device, you can upload the backed up configuration file to return to your previous settings. You can alternately upload the factory default configuration file if you want to return the device to the original default settings. The firmware determines the device's available features and functionality. You can download new firmware releases from your nearest ZyXEL FTP site (or www.zyxel.com) to use to upgrade your device's performance.

Only use firmware for your device's specific model. Refer to the label on the bottom of your ZyXEL Device.

22.1.1 What You Can Do in this Chapter

- Use the **Firmware** screen (Section 22.2 on page 255) to upload firmware to your device.
- Use the **Configuration** screen (Section 22.3 on page 256) to backup and restore device configurations. You can also reset your device settings back to the factory default.
- Use the **Restart** screen (Section 22.4 on page 259) to restart your ZyXEL device.

22.1.2 What You Need To Know

The following terms and concepts may help as you read this chapter.

Filename Conventions

The configuration file (often called the romfile or rom-0) contains the factory default settings in the menus such as password, DHCP Setup, and TCP/IP Setup. It arrives from ZyXEL with a "rom" filename extension. Once you have customized

the ZyXEL Device's settings, they can be saved back to your computer under a filename of your choosing.

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file "firmware.bin" to the ZyXEL Device.

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the ZyXEL Device only recognizes “rom-0” and “ras”. Be sure you keep unaltered copies of both files for later use.

The following table is a summary. Please note that the internal filename refers to the filename on the ZyXEL Device and the external filename refers to the filename not on the ZyXEL Device, that is, on your computer, local network and so the name (but not the extension) may vary. After uploading new firmware, see the **Status** screen to confirm that you have uploaded the correct firmware version.

Table 79 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	Rom-0	This is the configuration filename on the ZyXEL Device. Uploading the rom-0 file replaces the entire ROM file system, including your ZyXEL Device configurations, system-related data (including the default password), the error log and the trace log.	*.rom
Firmware	Ras	This is the generic name for the firmware on the ZyXEL Device.	*.bin

FTP Restrictions

FTP will not work when:

1. You are not logged on to the ZyXEL Device as an administrator (username ‘admin’).
2. The firewall is active (turn the firewall off or create a firewall rule to allow access from the WAN).
3. You have disabled the FTP service in the **Advanced > Service Control** screen.

22.1.3 Before You Begin

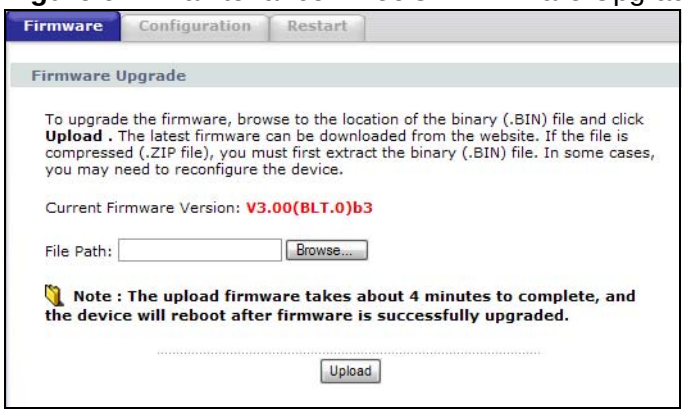
- Ensure you have either created a firewall rule to allow access from the WAN or turned the firewall off, otherwise the FTP will not function.
- Make sure the FTP service has not been disabled in the **Advanced > Service Control** screen.

22.2 Firmware Upgrade Screen

Click **Maintenance > Tools** to open the **Firmware** screen. Follow the instructions in this screen to upload firmware to your ZyXEL Device. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot. See Section 22.5.1 on page 260 for upgrading firmware using FTP/TFTP commands.

Do NOT turn off the ZyXEL Device while firmware upload is in progress!

Figure 92 Maintenance > Tools > Firmware Upgrade


Firmware
Configuration
Restart
Firmware Upgrade
To upgrade the firmware, browse to the location of the binary (.BIN) file and click Upload . The latest firmware can be downloaded from the website. If the file is compressed (.ZIP file), you must first extract the binary (.BIN) file. In some cases, you may need to reconfigure the device.
Current Firmware Version: V3.00(BLT.0)b3
File Path:
Browse...
Note : The upload firmware takes about 4 minutes to complete, and the device will reboot after firmware is successfully upgraded.
Upload

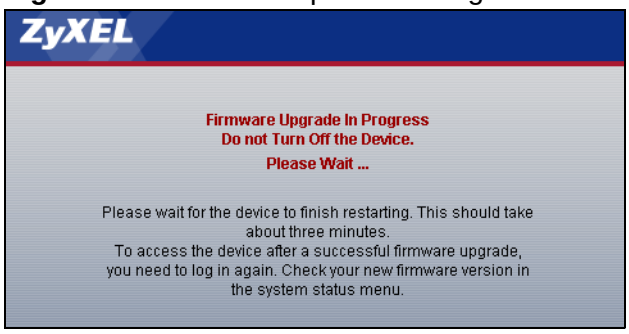
The following table describes the labels in this screen.

Table 80 Maintenance > Tools > Firmware Upgrade

LABEL	DESCRIPTION
Current Firmware Version	This is the present Firmware version and the date created.
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.

After you see the **Firmware Upload in Progress** screen, wait two minutes before logging into the ZyXEL Device again.

Figure 93 Firmware Upload In Progress


ZyXEL
Firmware Upgrade In Progress
Do not Turn Off the Device.
Please Wait ...
Please wait for the device to finish restarting. This should take about three minutes.
To access the device after a successful firmware upgrade, you need to log in again. Check your new firmware version in the system status menu.

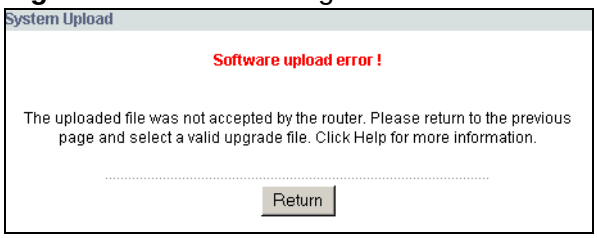
The ZyXEL Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 94 Network Temporarily Disconnected

After two minutes, log in again and check your new firmware version in the **Status** screen.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Firmware** screen.

Figure 95 Error Message

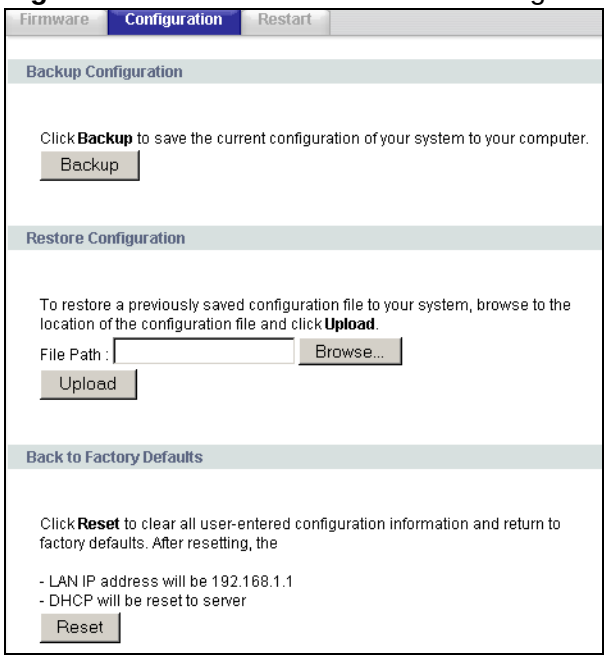

System Upload
Software upload error !
The uploaded file was not accepted by the router. Please return to the previous page and select a valid upgrade file. Click Help for more information.
Return

22.3 The Configuration Screen

See Section 22.5 on page 260 for transferring configuration files using FTP/TFTP commands.

Click **Maintenance > Tools > Configuration**. Information related to factory defaults, backup configuration, and restoring configuration appears in this screen, as shown next.

Figure 96 Maintenance > Tools > Configuration


Firmware
Configuration
Restart
Backup Configuration
Click Backup to save the current configuration of your system to your computer.
Backup
Restore Configuration
To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.
File Path :
Browse...
Upload
Back to Factory Defaults
Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the
- LAN IP address will be 192.168.1.1
- DHCP will be reset to server
Reset

Backup Configuration

Backup Configuration allows you to back up (save) the ZyXEL Device's current configuration to a file on your computer. Once your ZyXEL Device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the ZyXEL Device's current configuration to your computer.

Restore Configuration

Restore Configuration allows you to upload a new or previously saved configuration file from your computer to your ZyXEL Device.

Table 81 Restore Configuration

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click **Upload** to begin the upload process.

Do not turn off the ZyXEL Device while configuration file upload is in progress.

After you see a “restore configuration successful” screen, you must then wait one minute before logging into the ZyXEL Device again.

Figure 97 Configuration Upload Successful

ZyXEL
Router is restarting now.
Please wait ...
As there will be no indication of when the process is complete, please wait for two minute before attempting to access the router again.

The ZyXEL Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 98 Network Temporarily Disconnected

If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1). See Appendix B on page 305 for details on how to set up your computer’s IP address.

Reset to Factory Defaults

Click the **Reset** button to clear all user-entered configuration information and return the ZyXEL Device to its factory defaults. The following warning screen appears.

Figure 99 Reset Warning Message

Figure 100 Reset In Process Message

ZyXEL
Router is restarting now.
Please wait ...
As there will be no indication of when the process is complete, please wait for two minute before attempting to access the router again.

You can also press the **RESET** button on the rear panel to reset the factory defaults of your ZyXEL Device. Refer to Section 1.6 on page 26 for more information on the **RESET** button.

22.4 Restart

System restart allows you to reboot the ZyXEL Device without turning the power off.

Click **Maintenance > Tools** > **Restart**. Click **Restart** to have the ZyXEL Device reboot. This does not affect the ZyXEL Device's configuration.

Figure 101 Maintenance > Tools > Restart Screen

Firmware
Configuration
Restart
System Restart
Click Restart to have the device perform a software restart. The SYS LED blinks as the device restarts and then stays steady on if the restart is successful. Wait a minute before logging into the device again.
Restart

22.5 Technical Reference

The following section contains additional technical information about the ZyXEL Device features described in this chapter.

22.5.1 Tool Examples

Note: Only the administrator account (username 'admin') can access the ZyXEL Device through FTP.

Note: When uploading a firmware to the ZyXEL Device via TFTP/FTP, make sure you are in the 'FW' subdirectory. To do this while using an TFTP/FTP client, double-click the 'FW' folder. When using a command console, use the cd (change directory) command.

Using FTP or TFTP to Restore Configuration

This example shows you how to restore a previously saved configuration. Note that this function erases the current configuration before restoring a previous back up configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

FTP is the preferred method for restoring your current computer configuration to your device since FTP is faster. Please note that you must wait for the system to automatically restart after the file transfer is complete.

Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE your device. When the Restore Configuration process is complete, the device automatically restarts.

Restore Using FTP Session Example

Figure 102 Restore Using FTP Session Example

```
ftp> put config.rom rom-0
200 Port command okay
150 Opening data connection for STOR rom-0
226 File received OK
221 Goodbye for writing flash
ftp: 16384 bytes sent in 0.06Seconds 273.07Kbytes/sec.
ftp>quit
```

Refer to Section 22.1.2 on page 253 to read about configurations that disallow TFTP and FTP over WAN.

FTP and TFTP Firmware and Configuration File Uploads

These examples show you how to upload firmware and configuration files.

Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE your device.

FTP is the preferred method for uploading the firmware and configuration. To use this feature, your computer must have an FTP client. The following sections give examples of how to upload the firmware and the configuration files.

FTP File Upload Command from the DOS Prompt Example

1. Launch the FTP client on your computer.
2. Enter “open”, followed by a space and the IP address of your device.
3. Press [ENTER] when prompted for a username.
4. Enter your password as requested (the default is “1234”).
5. Enter “bin” to set transfer mode to binary.
6. Enter “cd fw” to open the firmware subdirectory.
7. Use “put” to transfer files from the computer to the device, for example, “put firmware.bin ras” transfers the firmware on your computer (firmware.bin) to the device and renames it “ras”. Similarly, “put config.rom rom-0” transfers the configuration file on your computer (config.rom) to the device and renames it “rom-0”. Likewise “get rom-0 config.rom” transfers the configuration file on the device to your computer and renames it “config.rom.” See earlier in this chapter for more information on filename conventions.
8. Enter “quit” to exit the ftp prompt.

FTP Session Example of Firmware File Upload

Below is an example of an FTP session.

Figure 103 FTP Session Example of Firmware File Upload

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> cd fw
250 OK. Current directory is /fw
ftp>put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 1103936 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

More commands (found in GUI-based FTP clients) are listed in this chapter.

Refer to Section 22.1.2 on page 253 to read about configurations that disallow TFTP and FTP over WAN.

TFTP File Upload

The device also supports the uploading of firmware files using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To transfer the firmware and the configuration file, follow the procedure shown next.

1. Use telnet from your computer to connect to the device and log in. Because TFTP does not have any security checks, the device records the IP address of the telnet client and accepts TFTP requests only from this address.
2. Enter the command “sys stdio 0” to disable the management idle timeout, so the TFTP transfer will not be interrupted. Enter “command sys stdio 5” to restore the five-minute management idle timeout (default) when the file transfer is complete.
3. Launch the TFTP client on your computer and connect to the device. Set the transfer mode to binary before starting data transfer.
4. Use the TFTP client (see the example below) to transfer files between the device and the computer. The file name for the firmware is “ras”.

Note that the telnet connection must be active and the device in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use “get” to transfer from the device to the computer, “put” the other way around, and “binary” to set binary transfer mode.

TFTP Upload Command Example

The following is an example TFTP command:

```
tftp [-i] host put firmware.bin ras
```

Where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the device’s IP address, “put” transfers the file source on the computer (firmware.bin – name of the firmware on the computer) to the file destination on the remote host (ras - name of the firmware on the device).

Commands that you may see in GUI-based TFTP clients are listed earlier in this chapter.

Configuration Backup Using GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

Table 82 General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

Refer to Section 22.1.2 on page 253 to read about configurations that disallow TFTP and FTP over WAN.

23

Diagnostic

23.1 Overview

These read-only screens display information to help you identify problems with the ZyXEL Device.

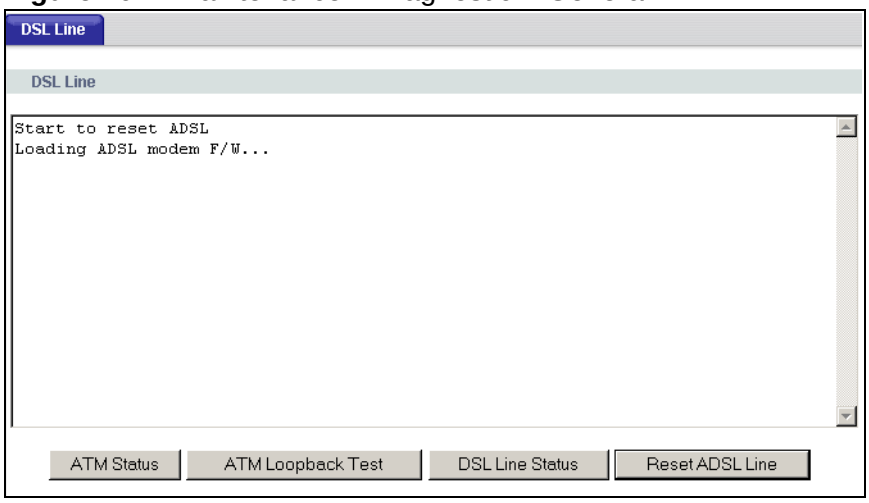
23.1.1 What You Can Do in the Diagnostic Screens

Use the **General Diagnostic** screen (Section 23.2 on page 265) to check or reset your DSL connection.

23.2 The General Diagnostic Screen

Click **Maintenance > Diagnostic** to open the screen shown next.

Figure 104 Maintenance > Diagnostic > General



The following table describes the fields in this screen.

Table 83 Maintenance > Diagnostic > General

ITEM	DESCRIPTION
ATM Status	Click this button to view your DSL connection's Asynchronous Transfer Mode (ATM) statistics. ATM is a networking technology that provides high-speed data transfer. ATM uses fixed-size packets of information called cells. With ATM, a high QoS (Quality of Service) can be guaranteed. The (Segmentation and Reassembly) SAR driver translates packets into ATM cells. It also receives ATM cells and reassembles them into packets. These counters are set back to zero whenever the device starts up. **inPkts** is the number of good ATM cells that have been received. **inDiscards** is the number of received ATM cells that were rejected. **outPkts** is the number of ATM cells that have been sent. **outDiscards** is the number of ATM cells sent that were rejected. **inF4Pkts** is the number of ATM Operations, Administration, and Management (OAM) F4 cells that have been received. See ITU recommendation I.610 for more on OAM for ATM. **outF4Pkts** is the number of ATM OAM F4 cells that have been sent. **inF5Pkts** is the number of ATM OAM F5 cells that have been received. **outF5Pkts** is the number of ATM OAM F5 cells that have been sent. **openChan** is the number of times that the ZyXEL Device has opened a logical DSL channel. **closeChan** is the number of times that the ZyXEL Device has closed a logical DSL channel. **txRate** is the number of bytes transmitted per second. **rxRate** is the number of bytes received per second.
ATM Loopback Test	Click this button to start the ATM loopback test. Make sure you have configured at least one PVC with proper VPIs/VCIs before you begin this test. The ZyXEL Device sends an OAM F5 packet to the DSLAM/ATM switch and then returns it (loops it back) to the ZyXEL Device. The ATM loopback test is useful for troubleshooting problems with the DSLAM and ATM network.

Table 83 Maintenance > Diagnostic > General

ITEM	DESCRIPTION
DSL Line Status	Click this button to view statistics about the DSL connections. **noise margin downstream** is the signal to noise ratio for the downstream part of the connection (coming into the ZyXEL Device from the ISP). It is measured in decibels. The higher the number the more signal and less noise there is. **output power upstream** is the amount of power (in decibels) that the ZyXEL Device is using to transmit to the ISP. **attenuation downstream** is the reduction in amplitude (in decibels) of the DSL signal coming into the ZyXEL Device from the ISP. Discrete Multi-Tone (DMT) modulation divides up a line's bandwidth into sub-carriers (sub-channels) of 4.3125 KHz each called tones. The rest of the display is the line's bit allocation. This is displayed as the number (in hexadecimal format) of bits transmitted for each tone. This can be used to determine the quality of the connection, whether a given sub-carrier loop has sufficient margins to support certain ADSL transmission rates, and possibly to determine whether particular specific types of interference or line attenuation exist. Refer to the ITU-T G.992.1 recommendation for more information on DMT. The better (or shorter) the line, the higher the number of bits transmitted for a DMT tone. The maximum number of bits that can be transmitted per DMT tone is 15. There will be some tones without any bits as there has to be space between the upstream and downstream channels.

Reset ADSL Line	Click this button to reinitialize the ADSL line. The large text box above then displays the progress and results of this operation, for example:
	
	`"Start to reset ADSL`
	
	`Loading ADSL modem F/W...`
	
	`Reset ADSL Line Successfully!"`

24

Account

24.1 Overview

Use this screen to change the password for the Administrator and User accounts for your ZyXEL Device.

24.2 Admin/Account Screen

Use this screen to change the password for the Administrator and User accounts for your ZyXEL Device.

Click **Maintenance > Account** to open the screen shown next.

Figure 105 Maintenance > Account > Admin

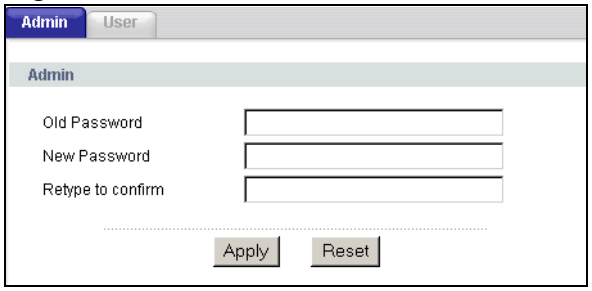
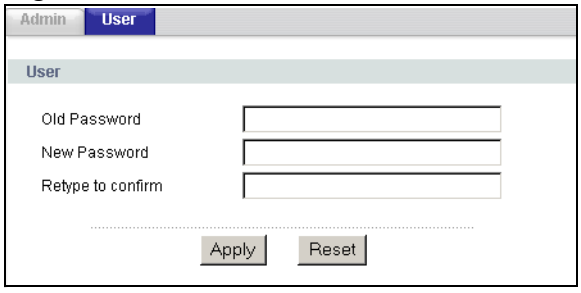


Figure 106 Maintenance > Account > User



The following table describes the labels in this screen.

Table 84 Maintenance > Account > Admin/User

ITEM	DESCRIPTION
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the ZyXEL Device.
Retype to Confirm	Type the new password again for confirmation.
Apply	Click this to save your changes back to the ZyXEL Device.
Cancel	Click this to begin configuring this screen afresh.

25

Troubleshooting

25.1 Overview

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- ZyXEL Device Access and Login
- Internet Access
- Phone Calls and VoIP
- Multiple SIP Accounts
- USB Device Connection

25.2 Power, Hardware Connections, and LEDs

The ZyXEL Device does not turn on. None of the LEDs turn on.

1. Make sure the ZyXEL Device is turned on.
2. Make sure you are using the power adaptor or cord included with the ZyXEL Device.
3. Make sure the power adaptor or cord is connected to the ZyXEL Device and plugged in to an appropriate power source. Make sure the power source is turned on.
4. Turn the ZyXEL Device off and on.
5. If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 1.5 on page 24.
2. Check the hardware connections. See the Quick Start Guide.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.
4. Turn the ZyXEL Device off and on.
5. If the problem continues, contact the vendor.

25.3 ZyXEL Device Access and Login

I forgot the IP address for the ZyXEL Device.

1. The default IP address is 192.168.1.1.
2. If you changed the IP address and have forgotten it, you might get the IP address of the ZyXEL Device by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the ZyXEL Device (it depends on the network), so enter this IP address in your Internet browser.
3. If this does not work, you have to reset the device to its factory defaults. See Section 1.6 on page 26.

I cannot see or access the **Login** screen in the web configurator.

1. Make sure you are using the correct IP address.
   - The default IP address is 192.168.1.1.
   - If you changed the IP address (Section on page 127), use the new IP address.

- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the ZyXEL Device.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.

3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See Appendix C on page 335.

4 Reset the device to its factory defaults, and try to access the ZyXEL Device with the default IP address. See Section 1.6 on page 26.

5 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the ZyXEL Device using another service, such as Telnet. If you can access the ZyXEL Device, check the remote management settings and firewall rules to find out why the ZyXEL Device does not respond to HTTP.
- If your computer is connected to the **WAN** port or is connected wirelessly, use a computer that is connected to a **ETHERNET** port.

I can see the **Login** screen, but I cannot log in to the ZyXEL Device.

1 Make sure you have entered the user name and password correctly. The default user name is **admin**. These fields are case-sensitive, so make sure [Caps Lock] is not on.

2 You cannot log in to the web configurator while someone is using Telnet to access the ZyXEL Device. Log out of the ZyXEL Device in the other session, or ask the person who is logged in to log out.

3 Turn the ZyXEL Device off and on.

4 If this does not work, you have to reset the device to its factory defaults. See Section 25.2 on page 271.

I cannot Telnet to the ZyXEL Device.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

I cannot use FTP to upload / download the configuration file. / I cannot use FTP to upload new firmware.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

25.4 Internet Access

I cannot access the Internet.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.5 on page 24.
2. Make sure you entered your ISP account information correctly. These fields are case-sensitive, so make sure [Caps Lock] is not on.
3. If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.
4. Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
5. If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the ZyXEL Device), but my Internet connection is not available anymore.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.5 on page 24.
2. Turn the ZyXEL Device off and on.
3. If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

1. There might be a lot of traffic on the network. Look at the LEDs, and check Section 1.5 on page 24. If the ZyXEL Device is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
2. Check the signal strength. If the signal strength is low, try moving the ZyXEL Device closer to the AP if possible, and look around to see if there are any devices that might be interfering with the wireless network (for example, microwaves, other wireless networks, and so on).
3. Turn the ZyXEL Device off and on.
4. If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

   Advanced Suggestions

   - Check the settings for QoS. If it is disabled, you might consider activating it. If it is enabled, you might consider raising or lowering the priority for some applications.

25.5 Phone Calls and VoIP

The telephone port won't work or the telephone lacks a dial tone.

1. Check the telephone connections and telephone wire.

I can access the Internet, but cannot make VoIP calls.

1. The **PHONE** light should come on. Make sure that your telephone is connected to the **PHONE** port.
2. You can also check the VoIP status in the **Status** screen.

3 If the VoIP settings are correct, use speed dial to make peer-to-peer calls. If you can make a call using speed dial, there may be something wrong with the SIP server, contact your VoIP service provider.

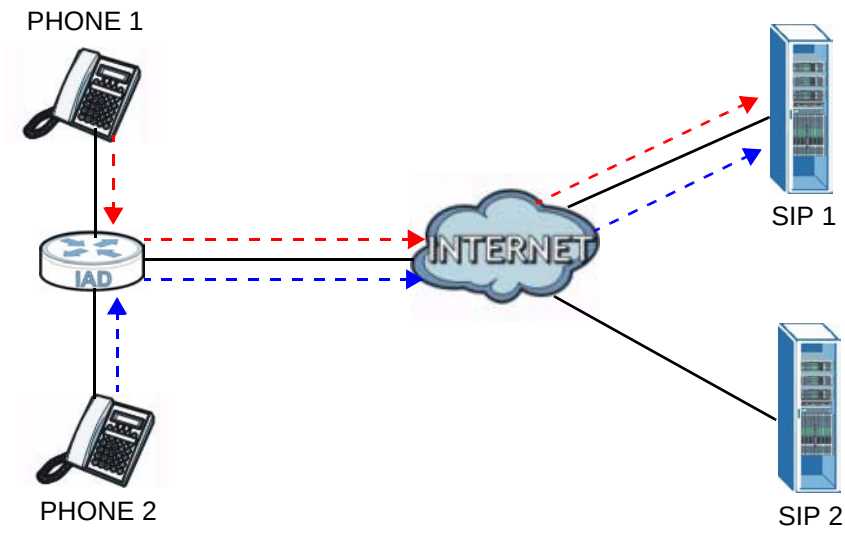
25.6 Multiple SIP Accounts

You can set up two SIP accounts on your ZyXEL Device and your ZyXEL Device is equipped with two phone ports. By default your ZyXEL Device uses SIP account 1 with both phone ports for outgoing calls, and it uses SIP accounts 1 and 2 for incoming calls. With this setting, you always use SIP account 1 for your outgoing calls and you cannot distinguish which SIP account the calls are coming in through. If you want to control the use of different dialing plans for accounting purposes or other reasons, you need to configure your phone ports in order to control which SIP account you are using when placing or receiving calls.

25.6.1 Outgoing Calls

The following figure represents the default behavior of your ZyXEL Device when two SIP accounts are configured and you are using two phones. When you place a call from phone port 1 or phone port 2, the ZyXEL Device will use SIP account 1.

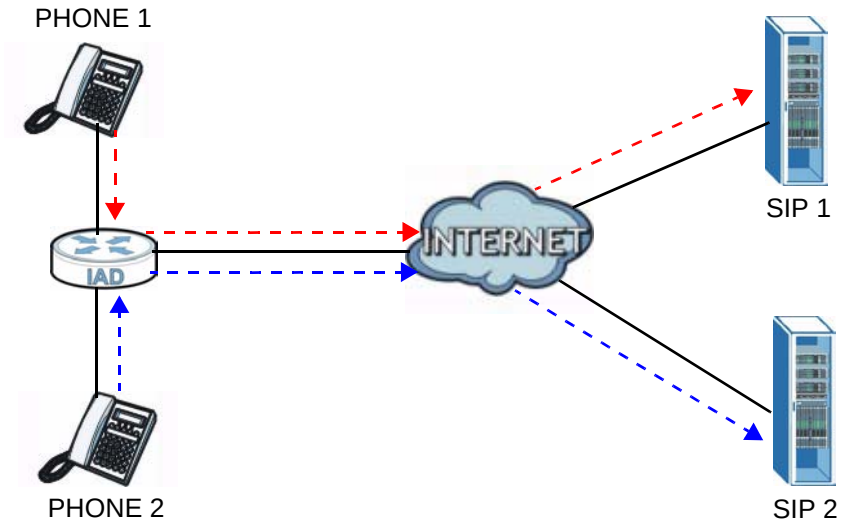
Figure 107 Outgoing Calls: Default



In the next example, phone port 1 is configured to use SIP account 1 and phone port 2 is configured to use SIP account 2. In this case, every time you place a call through phone port 1, you are using your SIP account 1. Similarly, every time you place a call through phone port 2, you are using your SIP account 2. To apply

these configuration changes you need to configure the **Analog Phone** screen. See Section 9.4 on page 169.

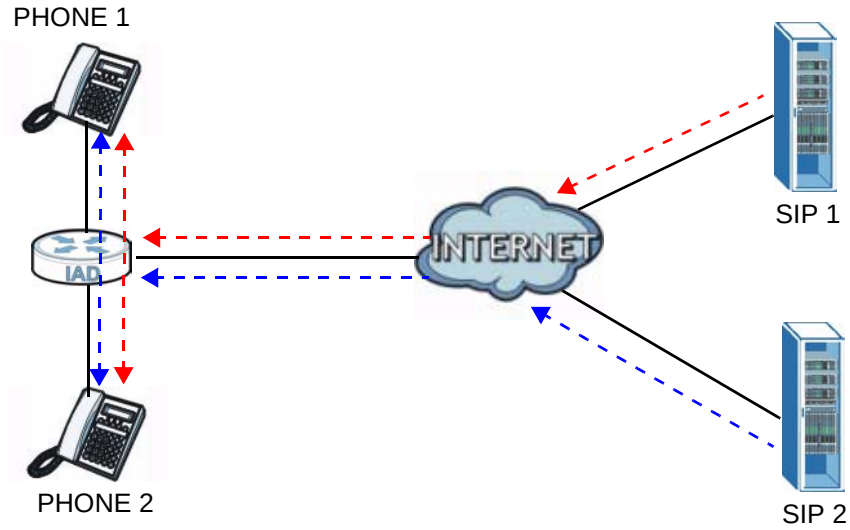
Figure 108 Outgoing Calls: Individual Configuration



25.6.2 Incoming Calls

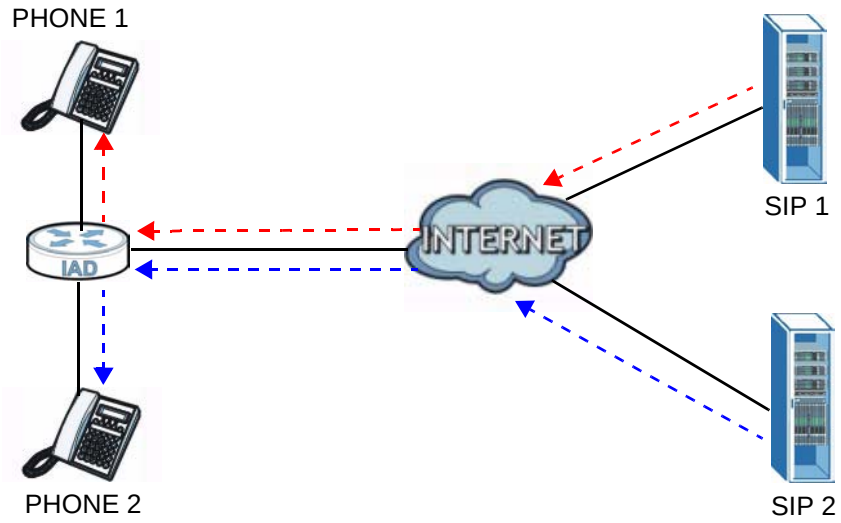
The following example shows the default behavior of your ZyXEL Device for incoming calls when two SIP accounts are configured and you are using two phones. When a call comes in from your SIP account 1, the phones connected to both phone port 1 and phone port 2 ring. Similarly, when a call comes in from your SIP account 2, the phones connected to both phone port 1 and phone port 2 ring. In either case you are not sure which SIP account the call is coming from.

Figure 109 Incoming Calls: Default



In the next example, phone port 1 is configured to use SIP account 1 and phone port 2 is configured to use SIP account 2 for incoming calls. In this case, every time you receive a call from your SIP account 1, the phone connected to phone port 1 rings. Similarly, every time you receive a call from your SIP account 2, phone port 2 rings. To apply these configuration changes you need to configure the **Analog Phone** screen. See Section 9.4 on page 169.

Figure 110 Incoming Calls: Individual Configuration



25.7 USB Device Connection

The ZyXEL Device fails to detect my USB device.

1. Disconnect the USB device.
2. Reboot the ZyXEL Device.
3. If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.
4. Re-connect your USB device to the ZyXEL Device.

26

Product Specifications

The following tables summarize the ZyXEL Device's hardware and firmware features.

Hardware Specifications

Table 85 Hardware Specifications

Dimensions	256 (W) x 145 (D) x 40 (H) mm
Weight	457 g
Power Specification	12V 1.5A DC
Built-in Switch	Four auto-negotiating, auto MDI/MDI-X 10/100/1000 Mbps RJ-45 Ethernet ports
DSL Port	P-2612HNU-F1: One RJ-11 DSL port P-2612HNU-F3: One RJ-45 DSL port
WAN Port	One RJ-45 WAN port
PHONE Ports	2 RJ-11 FXS POTS ports
RESET Button	Restores factory defaults
WLAN/WPS Button	1 second: Turn on or off WLAN 5 seconds: Start WPS
USB Port	Two USB v2.0 ports for file sharing or print server setup
Antenna	Two 2 dBi external fixed antennas, 2 x 2
Operation Temperature	0º C ~ 40º C
Storage Temperature	-20º ~ 60º C
Operation Humidity	20% ~ 85% RH
Storage Humidity	20% ~ 90% RH
Distance between the centers of the holes (for wall-mounting) on the device's back	137.20mm
Screw size for wall-mounting	M4 tap

Firmware Specifications

Table 86 Firmware Specifications

Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)
Default User Name	admin
Default Password	1234
DHCP Server IP Pool	Starting Address: 192.168.1.33 Size: 32
Static DHCP Addresses	10
Static Routes	16
Device Management	Use the web configurator to easily configure the rich range of features on the ZyXEL Device.
Wireless Functionality (wireless devices only)	Allow the IEEE 802.11n, IEEE 802.11b and/or IEEE 802.11g wireless clients to connect to the ZyXEL Device wirelessly. Enable wireless security (WEP, WPA(2), WPA(2)-PSK) and/or MAC filtering to protect your wireless network.
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the web configurator, an HTTP/FTP/SCP/SFTP tool to put it on the ZyXEL Device. Note: Only upload firmware for your specific model!
Configuration Backup & Restoration	Make a copy of the ZyXEL Device's configuration. You can put it back on the ZyXEL Device later if you decide to revert back to an earlier configuration.
Network Address Translation (NAT)	Each computer on your network must have its own unique IP address. Use NAT to convert your public IP address(es) to multiple private IP addresses for the computers on your network.
Port Forwarding	If you have a server (mail or web server for example) on your network, you can use this feature to let people access it from the Internet.
IEEE 802.1Q and IEEE 802.1P	Use IEEE 802.1Q VLAN and IEEE 802.1P priority tags in implementing QoS. Configure VLANs based on port, PVC, and SSID. Specify a PVID to assign to untagged frames or priority-tagged frames received on this port, SSID, or PVC. Assign a priority for the traffic transmitted through a port, SSID, or PVC.
DHCP (Dynamic Host Configuration Protocol)	Use this feature to have the ZyXEL Device assign IP addresses, an IP default gateway and DNS servers to computers on your network. Your device can also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from the actual real DHCP server to the clients.
Dynamic DNS Support	With Dynamic DNS (Domain Name System) support, you can use a fixed URL, www.zyxel.com for example, with a dynamic IP address. You must register for this service with a Dynamic DNS service provider.

Table 86 Firmware Specifications (continued)

IP Multicast	IP multicast is used to send traffic to a specific group of computers. The ZyXEL Device supports versions 1 and 2 of IGMP (Internet Group Management Protocol) used to join multicast groups (see RFC 2236).
Time and Date	Get the current time and date from an external server when you turn on your ZyXEL Device. You can also set the time manually. These dates and times are then used in logs.
Logs	Use logs for troubleshooting. You can send logs from the ZyXEL Device to an external syslog server.
Universal Plug and Play (UPnP)	A UPnP-enabled device can dynamically join a network, obtain an IP address and convey its capabilities to other devices on the network.
Firewall	Your device has a stateful inspection firewall with DoS (Denial of Service) protection. By default, when the firewall is activated, all incoming traffic from the WAN to the LAN is blocked unless it is initiated from the LAN. The firewall supports TCP/UDP inspection, DoS detection and prevention, real time alerts, reports and logs.
QoS (Quality of Service)	You can efficiently manage traffic on your network by reserving bandwidth and giving priority to certain types of traffic and/or to particular computers.
Remote Management	This allows you to decide whether a service (HTTP or FTP traffic for example) from a computer on a network (LAN or WAN for example) can access the ZyXEL Device.
PPPoE Support (RFC2516)	PPPoE (Point-to-Point Protocol over Ethernet) emulates a dial-up connection. It allows your ISP to use their existing network configuration with newer broadband technologies such as ADSL. The PPPoE driver on your device is transparent to the computers on the LAN, which see only Ethernet and are not aware of PPPoE thus saving you from having to manage PPPoE clients on individual computers.
Other PPPoE Features	PPPoE idle time out PPPoE dial on demand
Multiple PVC (Permanent Virtual Circuits) Support	Your device supports one Permanent Virtual Circuits (PVCs).
Packet Filters	Your device's packet filtering function allows added network security and management.

Table 86 Firmware Specifications (continued)

ADSL Standards	Support ITU G.992.1 G.dmt EOC specified in ITU-T G.992.1 ADSL2 G.dmt.bis (G.992.3) ADSL 2/2+ AnnexM ADSL2+ (G.992.5) Reach-Extended ADSL (RE ADSL) SRA (Seamless Rate Adaptation) Auto-negotiating rate adaptation ADSL physical connection AAL5 (ATM Adaptation Layer type 5) Multi-protocol over AAL5 (RFC 2684) PPP over ATM AAL5 (RFC 2364) PPP over Ethernet (RFC 2516) Multiple PPPoE VC-based and LLC-based multiplexing I.610 F4/F5 OAM
Other Protocol Support	PPP (Point-to-Point Protocol) link layer protocol Transparent bridging for unsupported network layer protocols RIP I/RIP II ICMP ATM QoS SNMP v1 and v2c with MIB II support (RFC 1213) IP Multicasting IGMP v1 and v2 IGMP Proxy
Management	Embedded Web Configurator CLI (Command Line Interpreter) SNMP v1 & v2c with MIB II Firmware upgrade and configuration file restore through Web/FTP/SCP/SFTP Telnet for remote management Remote Management Control: Telnet, FTP, Web, SNMP and DNS. Remote Firmware Upgrade Syslog

Voice Specifications

Note: To take full advantage of the supplementary phone services available through the ZyXEL Device's phone port, you may need to subscribe to the services from your VoIP service provider.

Note: Not all features are supported by all service providers. Consult your service provider for more information.

Table 87 Voice Features

Call Park and Pickup	Call park and pickup lets you put a call on hold (park) and then continue the call (pickup). The caller must still pay while the call is parked. When you park the call, you enter a number of your choice (up to eight digits), which you must enter again when you pick up the call. If you do not enter the correct number, you cannot pickup the call. This means that only someone who knows the number you have chosen can pick up the call. You can have more than one call on hold at the same time, but you must give each call a different number.
Call Return	With call return, you can place a call to the last number that called you (either answered or missed). The last incoming call can be through either SIP or PSTN.
Country Code	Phone standards and settings differ from one country to another, so the settings on your ZyXEL Device must be configured to match those of the country you are in. The country code feature allows you to do this by selecting the country from a list rather than changing each setting manually. Configure the country code feature when you move the ZyXEL Device from one country to another.
Do not Disturb (DnD)	This feature allows you to set your phone not to ring when someone calls you. You can set each phone independently using its keypad, or configure global settings for all phones using the command line interpreter.
Auto Dial	You can set the ZyXEL Device to automatically dial a specified number immediately whenever you lift a phone off the hook. Use the Web Configurator to set the specified number. Use the command line interpreter to have the ZyXEL Device wait a specified length of time before dialing the number.
Phone config	The phone config table allows you to customize the phone keypad combinations you use to access certain features on the ZyXEL Device, such as call waiting, call return, and call forward. The phone config table is configurable in command interpreter mode.
HTTP pincode	If your service provider uses an auto provisioning server, you need to enter a personal identification number (supplied by your service provider) before you first use the feature.

Table 87 Voice Features

Firmware update enable / disable	If your service provider uses this feature, you hear a recorded message when you pick up the phone when new firmware is available for your ZyXEL Device. Enter *99# in your phone's keypad to have the ZyXEL Device upgrade the firmware, or enter #99# to not upgrade. If your service provider gave you different numbers to use, enter them instead. If you enter the code to not upgrade, you can make a call as normal. You will hear the recording again each time you pick up the phone, until you upgrade.
Call waiting	This feature allows you to hear an alert when you are already using the phone and another person calls you. You can then either reject the new incoming call, put your current call on hold and receive the new incoming call, or end the current call and receive the new incoming call.
Call forwarding	With this feature, you can set the ZyXEL Device to forward calls to a specified number, either unconditionally (always), when your number is busy, or when you do not answer. You can also forward incoming calls from one specified number to another.
Caller ID	The ZyXEL Device supports caller ID, which allows you to see the originating number of an incoming call (on a phone with a suitable display).
REN	A Ringer Equivalence Number (REN) is used to determine the number of devices (like telephones or fax machines) that may be connected to the telephone line. Your device has a REN of three, so it can support three devices per telephone port.
Dynamic Jitter Buffer	The built-in adaptive buffer helps to smooth out the variations in delay (jitter) for voice traffic. This helps ensure good voice quality for your conversations.
Multiple SIP Accounts	You can simultaneously use multiple voice (SIP) accounts and assign them to the telephone port.
Multiple Voice Channels	Your device can simultaneously handle multiple voice channels (telephone calls). Additionally you can answer an incoming phone call on a VoIP account, even while someone else is using the account for a phone call.
Voice Activity Detection/Silence Suppression	Voice Activity Detection (VAD) reduces the bandwidth that a call uses by not transmitting when you are not speaking.
Comfort Noise Generation	Your device generates background noise to fill moments of silence when the other device in a call stops transmitting because the other party is not speaking (as total silence could easily be mistaken for a lost connection).
Echo Cancellation	You device supports G.168, an ITU-T standard for eliminating the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.
QoS (Quality of Service)	Quality of Service (QoS) mechanisms help to provide better service on a per-flow basis. Your device supports Type of Service (ToS) tagging and Differentiated Services (DiffServ) tagging. This allows the device to tag voice frames so they can be prioritized over the network.

Table 87 Voice Features

SIP ALG	Your device is a SIP Application Layer Gateway (ALG). It allows VoIP calls to pass through NAT for devices behind it (such as a SIP-based VoIP software application on a computer).
Other Voice Features	SIP version 2 (Session Initiation Protocol RFC 3261) SDP (Session Description Protocol RFC 2327) RTP (RFC 1889) RTCP (RFC 1890) Voice codecs (coder/decoders) G.711, G.729 Fax and data modem discrimination DTMF Detection and Generation DTMF: In-band and Out-band traffic (RFC 2833),(PCM), (SIP INFO) Point-to-point call establishment between two IADs Quick dialing through predefined phone book, which maps the phone dialing number and destination URL. Flexible Dial Plan (RFC3525 section 7.1.14)

Wireless Features

Table 88 Wireless Features

External Antenna	The ZyXEL Device is equipped with an attached antenna to provide a clear radio signal between the wireless stations and the access points.
Multiple SSID	Multiple SSID allows the ZyXEL Device to operate up to 4 different wireless networks simultaneously, each with independently configurable wireless and security settings.
WDS	WDS (Wireless Distribution System) lets the ZyXEL Device act as a bridge with other ZyXEL access points.
Wireless LAN MAC Address Filtering	Your device can check the MAC addresses of wireless stations against a list of allowed or denied MAC addresses.
WEP Encryption	WEP (Wired Equivalent Privacy) encrypts data frames before transmitting over the wireless network to help keep network communications private.
Wi-Fi Protected Access	Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i security standard. Key differences between WPA and WEP are user authentication and improved data encryption.
WPA2	WPA 2 is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Table 88 Wireless Features

WPS	Wi-Fi Protected Setup
Other Wireless Features	IEEE 802.11g Compliance Frequency Range: 2.4 GHz ISM Band Advanced Orthogonal Frequency Division Multiplexing (OFDM) Data Rates: 54Mbps, 11Mbps, 5.5Mbps, 2Mbps, and 1 Mbps Auto Fallback Turn on-off WLAN by **WLAN** button (press the **WLAN** button for one second to turn the WLAN on or turn off; five seconds to turn on WPS) IEEE 802.11i IEEE 802.11e Wired Equivalent Privacy (WEP) Data Encryption 64/128/256 bit. WLAN bridge to LAN Up to 32 MAC Address filters IEEE 802.1x External RADIUS server using EAP-MD5, TLS, TTLS Scheduling lets you set when the WLAN is on.

The following list, which is not exhaustive, illustrates the standards supported in the ZyXEL Device.

Table 89 Standards Supported

STANDARD	DESCRIPTION
RFC 867	Daytime Protocol
RFC 868	Time Protocol.
RFC 1058	RIP-1 (Routing Information Protocol)
RFC 1112	IGMP v1
RFC 1157	SNMPv1: Simple Network Management Protocol version 1
RFC 1305	Network Time Protocol (NTP version 3)
RFC 1441	SNMPv2 Simple Network Management Protocol version 2
RFC 1483	Multiprotocol Encapsulation over ATM Adaptation Layer 5
RFC 1631	IP Network Address Translator (NAT)
RFC 1661	The Point-to-Point Protocol (PPP)
RFC 1723	RIP-2 (Routing Information Protocol)
RFC 1901	SNMPv2c Simple Network Management Protocol version 2c
RFC 2236	Internet Group Management Protocol, Version 2.
RFC 2364	PPP over AAL5 (PPP over ATM over ADSL)

Table 89 Standards Supported (continued)

STANDARD	DESCRIPTION
RFC 2408	Internet Security Association and Key Management Protocol (ISAKMP)
RFC 2516	A Method for Transmitting PPP Over Ethernet (PPPoE)
RFC 2684	Multiprotocol Encapsulation over ATM Adaptation Layer 5.
RFC 2766	Network Address Translation - Protocol
IEEE 802.11	Also known by the brand Wi-Fi, denotes a set of Wireless LAN/ WLAN standards developed by working group 11 of the IEEE LAN/MAN Standards Committee (IEEE 802).
IEEE 802.11b	Uses the 2.4 gigahertz (GHz) band
IEEE 802.11g	Uses the 2.4 gigahertz (GHz) band
IEEE 802.11n	Uses the 2.4 gigahertz (GHz) band and 5 gigahertz (GHz) band
IEEE 802.11d	Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges
IEEE 802.11x	Port Based Network Access Control.
IEEE 802.11e QoS	IEEE 802.11 e Wireless LAN for Quality of Service
ANSI T1.413, Issue 2	Asymmetric Digital Subscriber Line (ADSL) standard.
G dmt(G.992.1)	G.992.1 Asymmetrical Digital Subscriber Line (ADSL) Transceivers
ITU G.992.1 (G.DMT)	ITU standard for ADSL using discrete multitone modulation.
ITU G.992.2 (G. Lite)	ITU standard for ADSL using discrete multitone modulation.
ITU G.992.3 (G.dmt.bis)	ITU standard (also referred to as ADSL2) that extends the capability of basic ADSL in data rates.
ITU G.992.4 (G.lite.bis)	ITU standard (also referred to as ADSL2) that extends the capability of basic ADSL in data rates.
ITU G.992.5 (ADSL2+)	ITU standard (also referred to as ADSL2+) that extends the capability of basic ADSL by doubling the number of downstream bits.
Microsoft PPTP	MS PPTP (Microsoft's implementation of Point to Point Tunneling Protocol)
RFC 2383	ST2+ over ATM Protocol Specification - UNI 3.1 Version
TR-069	TR-069 DSL Forum Standard for CPE Wan Management.
1.363.5	Compliant AAL5 SAR (Segmentation And Re-assembly)

Wall-mounting Instructions

Do the following to hang your ZyXEL Device on a wall.

Note: See Table 85 on page 279 for the size of screws to use and how far apart to place them.

1 Locate a high position on a wall that is free of obstructions. Use a sturdy wall.

2 Drill two holes for the screws. Make sure the distance between the centers of the holes matches what is listed in the product specifications appendix.

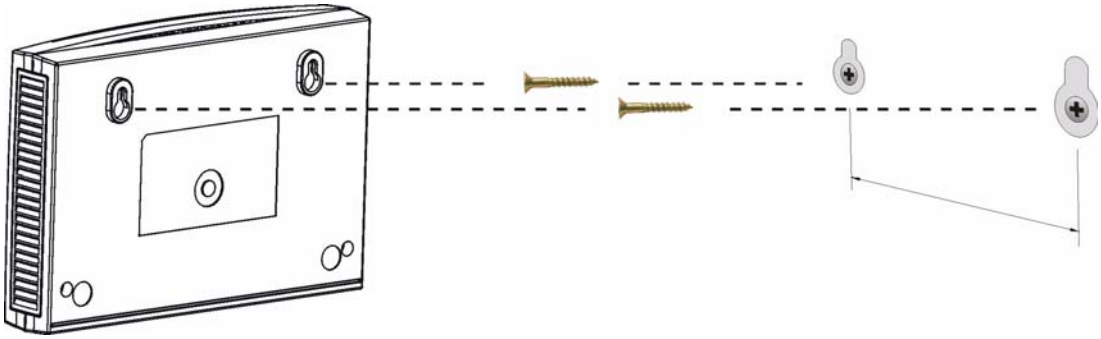
Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.

3 Do not screw the screws all the way into the wall. Leave a small gap of about 0.5 cm between the heads of the screws and the wall.

4 Make sure the screws are snugly fastened to the wall. They need to hold the weight of the ZyXEL Device with the connection cables.

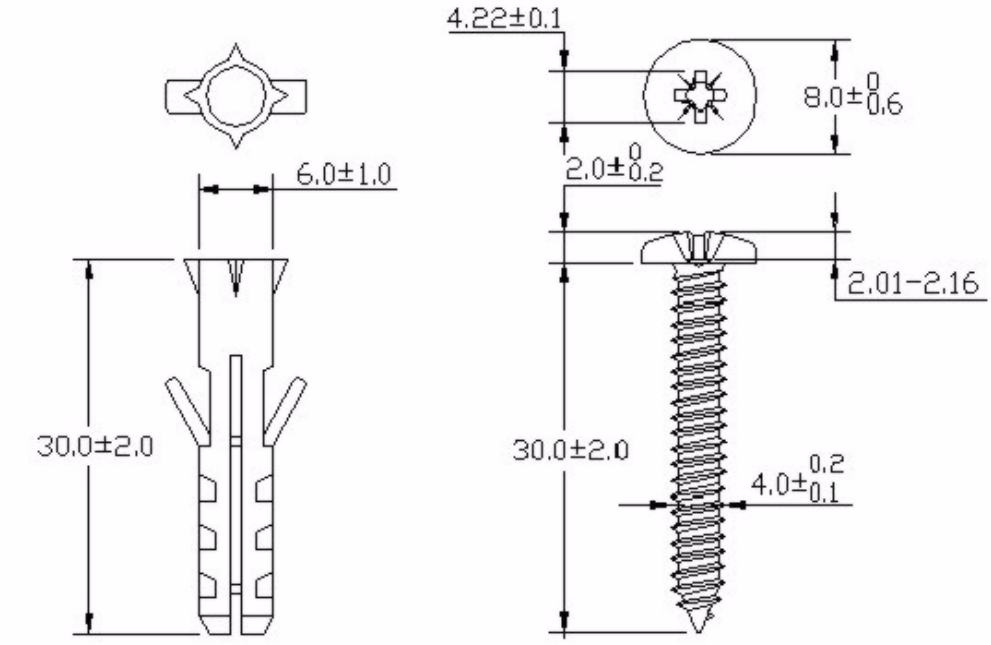
5 Align the holes on the back of the ZyXEL Device with the screws on the wall. Hang the ZyXEL Device on the screws.

Figure 111 Wall-mounting Example



The following are dimensions of an M4 tap screw and masonry plug used for wall mounting. All measurements are in millimeters (mm).

Figure 112 Masonry Plug and M4 Tap Screw



PART IV Appendices and Index

Setting Up Your Computer's IP Address (305)

Pop-up Windows, JavaScripts and Java Permissions (335)

IP Addresses and Subnetting (293)

Wireless LANs (345)

Common Services (369)

Open Software Announcements (373)

Legal Information (397)

Index (399)

A

IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (such as computers, servers, routers, and printers) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

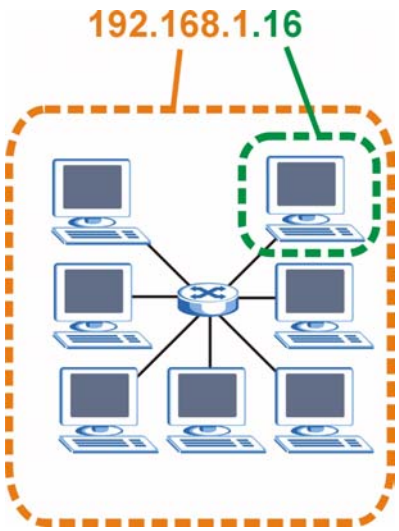
Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

Figure 113 Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term “subnet” is short for “sub-network”.

A subnet mask has 32 bits. If a bit in the subnet mask is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Table 90 IP Address Network Number and Host ID Example

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	**11111111**	**11111111**	**11111111**	00000000
Network Number	**11000000**	**10101000**	**00000001**	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a “1” value). For example, an “8-bit mask” means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

Table 91 Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 92 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} – 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} – 2$	65534
24 bits	255.255.255.0	8 bits	$2^{8} – 2$	254
29 bits	255.255.255.248	3 bits	$2^{3} – 2$	6

Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

Table 93 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

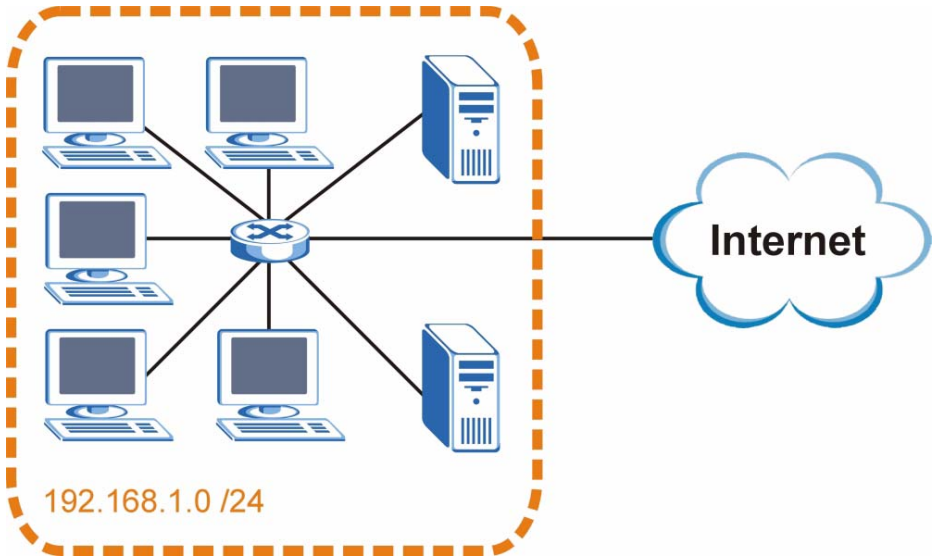
Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of 2^8 – 2 or 254 possible hosts.

The following figure shows the company network before subnetting.

Figure 114 Subnetting Example: Before Subnetting

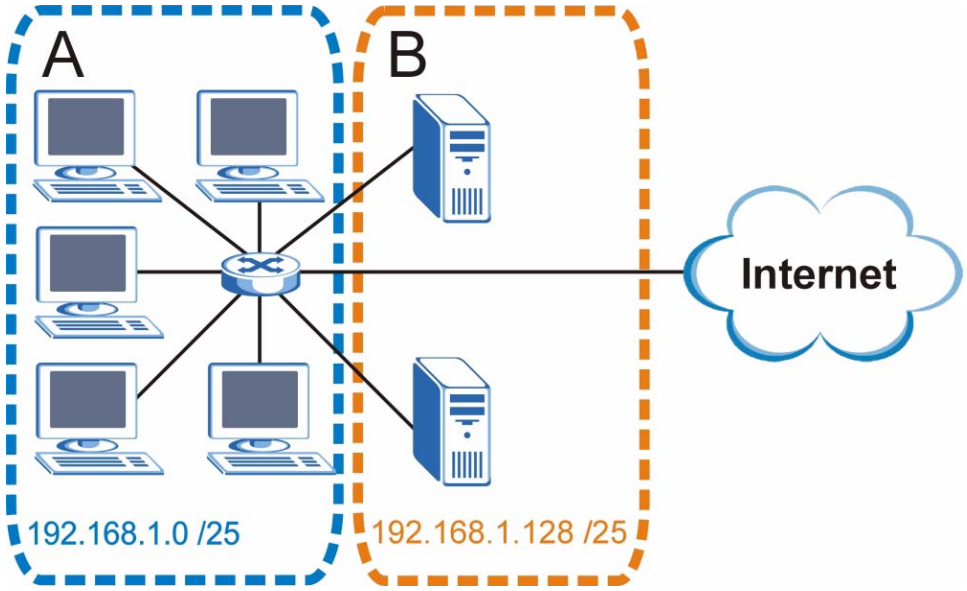


You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The “borrowed” host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

Figure 115 Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of $2^7 - 2$ or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving 2^6 - 2 or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Table 94 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 95 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 96 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 97 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

Table 98 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

Table 99 24-bit Network Number Subnet Planning

NO. “BORROWED” HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

Table 100 16-bit Network Number Subnet Planning

NO. “BORROWED” HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382

Table 100 16-bit Network Number Subnet Planning (continued)

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the ZyXEL Device.

Once you have decided on the network number, pick an IP address for your ZyXEL Device that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your ZyXEL Device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the ZyXEL Device unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space.

IP Address Conflicts

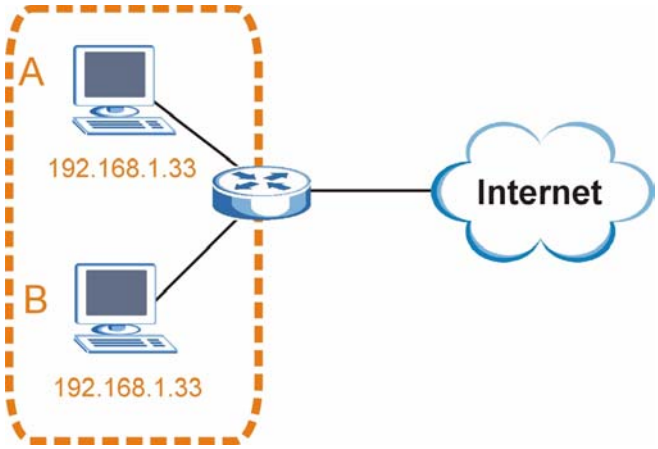
Each device on a network must have a unique IP address. Devices with duplicate IP addresses on the same network will not be able to access the Internet or other resources. The devices may also be unreachable through the network.

Conflicting Computer IP Addresses Example

More than one device can not use the same IP address. In the following example computer **A** has a static (or fixed) IP address that is the same as the IP address that a DHCP server assigns to computer **B** which is a DHCP client. Neither can access the Internet. This problem can be solved by assigning a different static IP

address to computer **A** or setting computer **A** to obtain an IP address automatically.

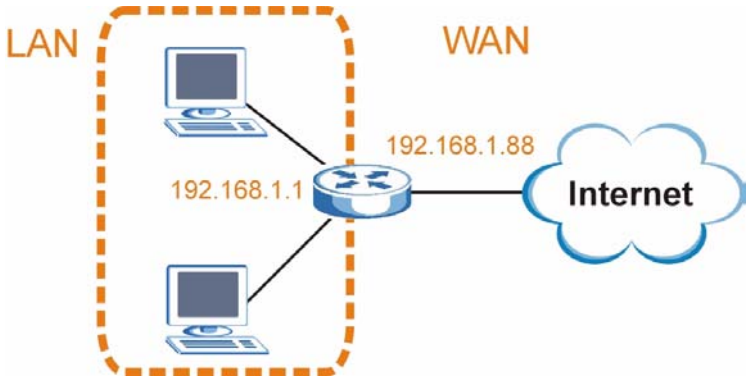
Figure 116 Conflicting Computer IP Addresses Example



Conflicting Router IP Addresses Example

Since a router connects different networks, it must have interfaces using different network numbers. For example, if a router is set between a LAN and the Internet (WAN), the router's LAN and WAN addresses must be on different subnets. In the following example, the LAN and WAN are on the same subnet. The LAN computers cannot access the Internet because the router cannot route between networks.

Figure 117 Conflicting Computer IP Addresses Example

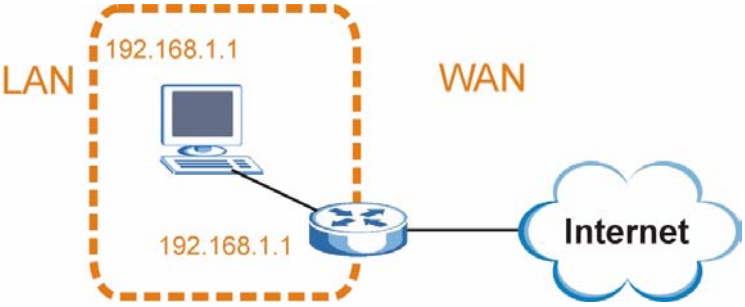


Conflicting Computer and Router IP Addresses Example

More than one device can not use the same IP address. In the following example, the computer and the router's LAN port both use 192.168.1.1 as the IP address.

The computer cannot access the Internet. This problem can be solved by assigning a different IP address to the computer or the router's LAN port.

Figure 118 Conflicting Computer and Router IP Addresses Example



B

Setting Up Your Computer's IP Address

Note: Your specific ZyXEL Device may not support all of the operating systems described in this appendix. See the product specifications for more information about which operating systems are supported.

This appendix shows you how to configure the IP settings on your computer in order for it to be able to communicate with the other devices on your network. Windows Vista/XP/2000, Mac OS 9/OS X, and all versions of UNIX/LINUX include the software components you need to use TCP/IP on your computer.

If you manually assign IP information instead of using a dynamic IP, make sure that your network's computers have IP addresses that place them in the same subnet.

In this appendix, you can set up an IP address for:

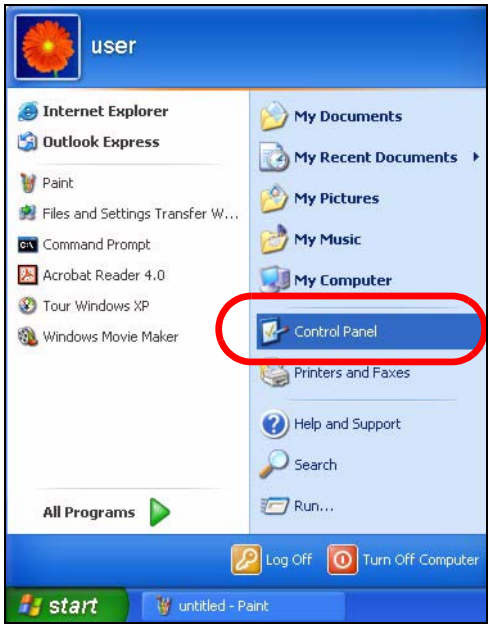
- Windows XP/NT/2000 on page 305
- Windows Vista on page 309
- Windows 7 on page 313
- Mac OS X: 10.3 and 10.4 on page 317
- Mac OS X: 10.5 on page 321
- Linux: Ubuntu 8 (GNOME) on page 324
- Linux: openSUSE 10.3 (KDE) on page 329

Windows XP/NT/2000

The following example uses the default Windows XP display theme but can also apply to Windows 2000 and Windows NT.

1 Click **Start** > **Control Panel**.

Figure 119 Windows XP: Start Menu

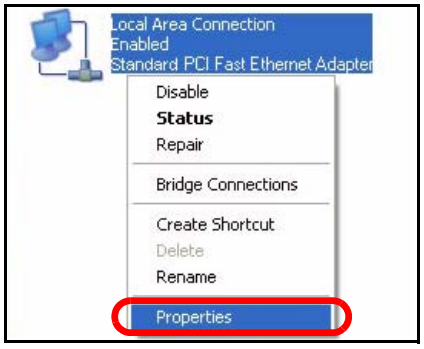


2 In the **Control Panel**, click the **Network Connections** icon.

Figure 120 Windows XP: Control Panel

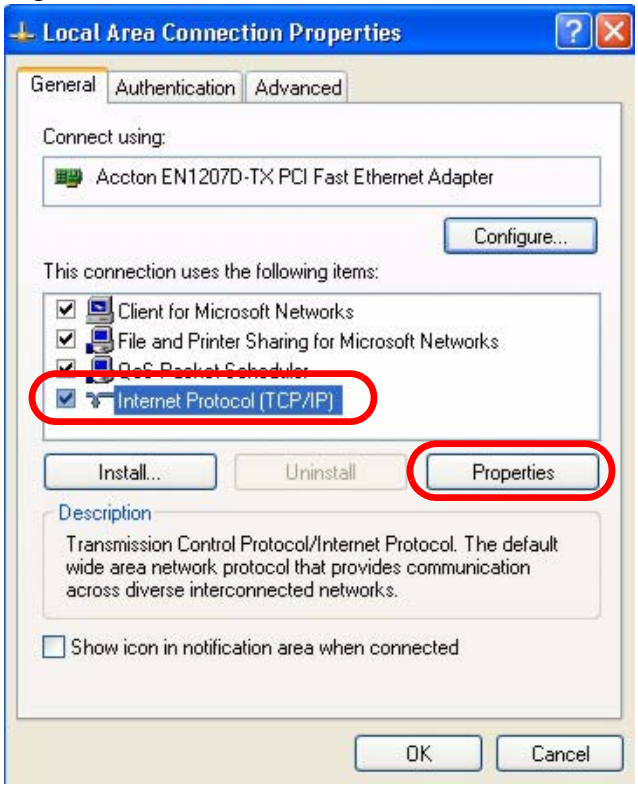
3 Right-click **Local Area Connection** and then select **Properties**.

Figure 121 Windows XP: Control Panel > Network Connections > Properties



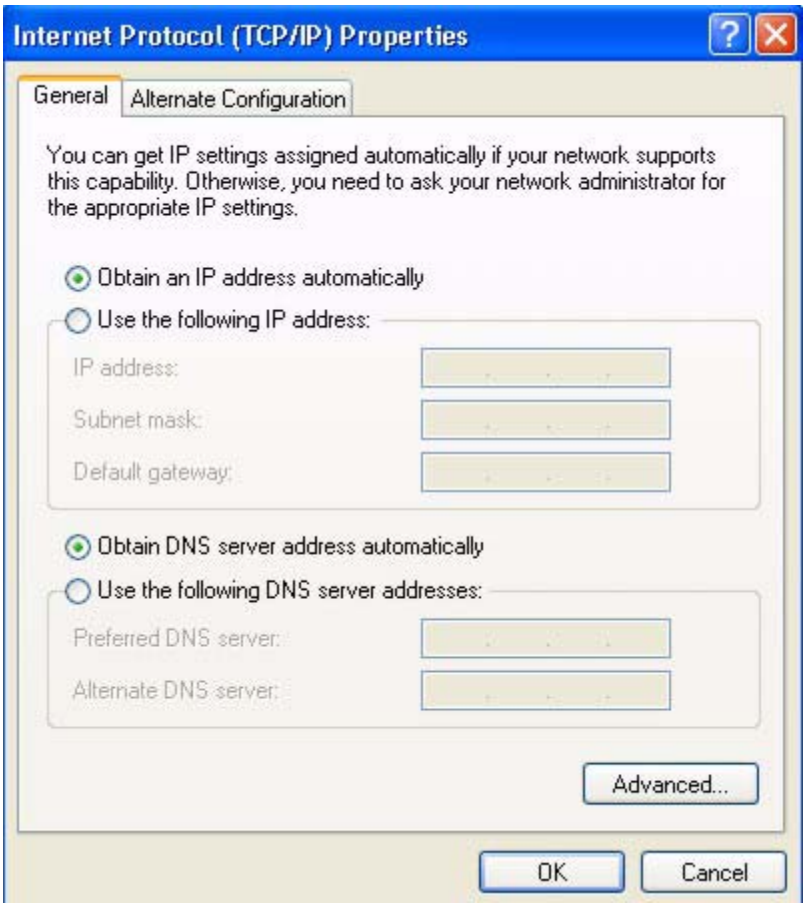
4 On the **General** tab, select **Internet Protocol (TCP/IP)** and then click **Properties**.

Figure 122 Windows XP: Local Area Connection Properties



5 The **Internet Protocol TCP/IP Properties** window opens.

Figure 123 Windows XP: Internet Protocol (TCP/IP) Properties


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

6 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided.

7 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

8 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

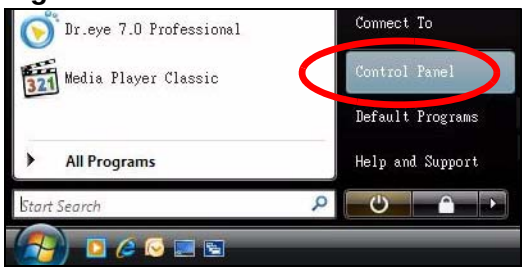
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

Windows Vista

This section shows screens from Windows Vista Professional.

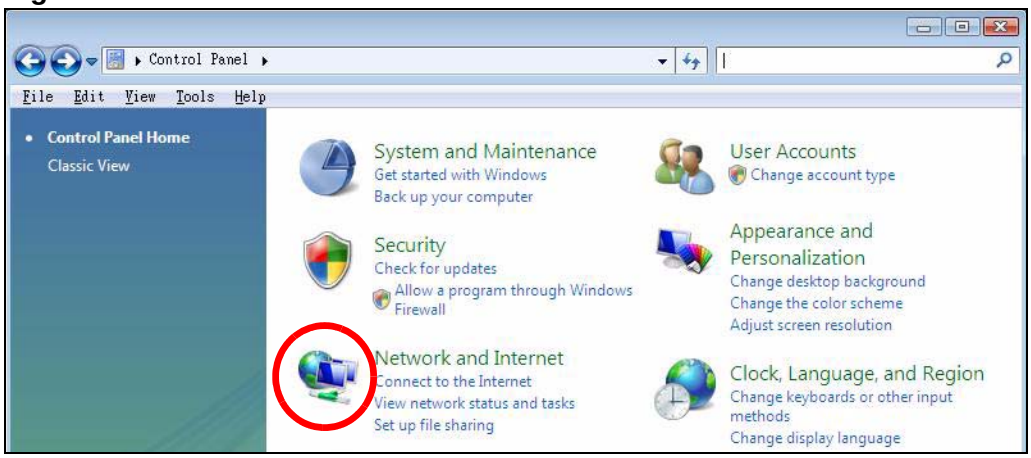
1 Click **Start** > **Control Panel**.

Figure 124 Windows Vista: Start Menu



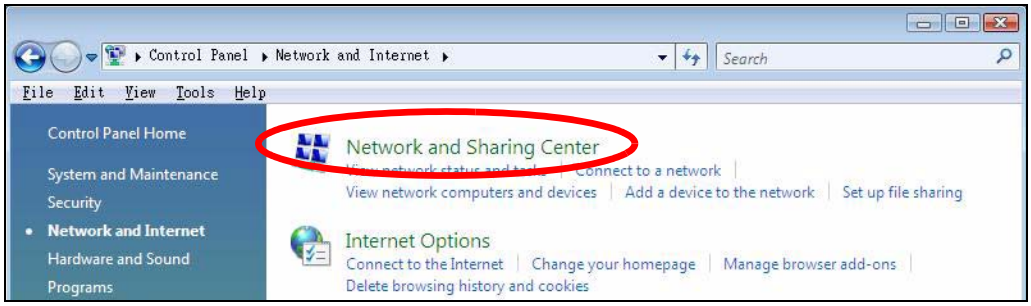
2 In the **Control Panel**, click the **Network and Internet** icon.

Figure 125 Windows Vista: Control Panel



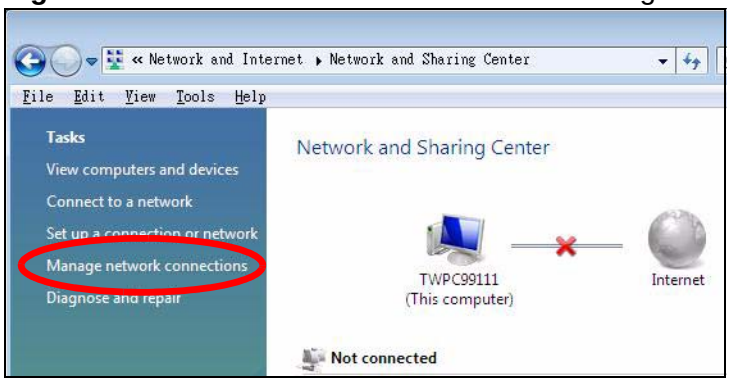
3 Click the **Network and Sharing Center** icon.

Figure 126 Windows Vista: Network And Internet



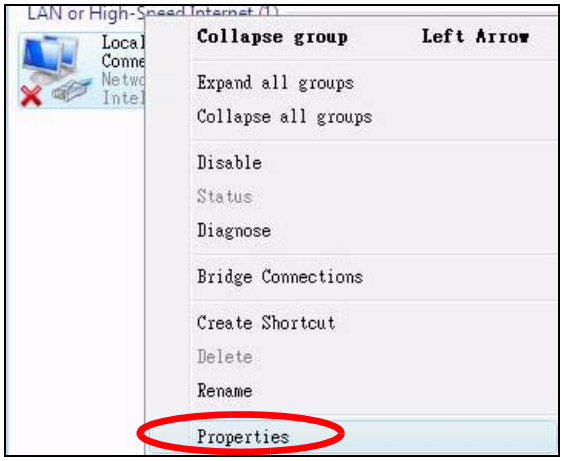
4 Click **Manage network connections**.

Figure 127 Windows Vista: Network and Sharing Center



5 Right-click **Local Area Connection** and then select **Properties**.

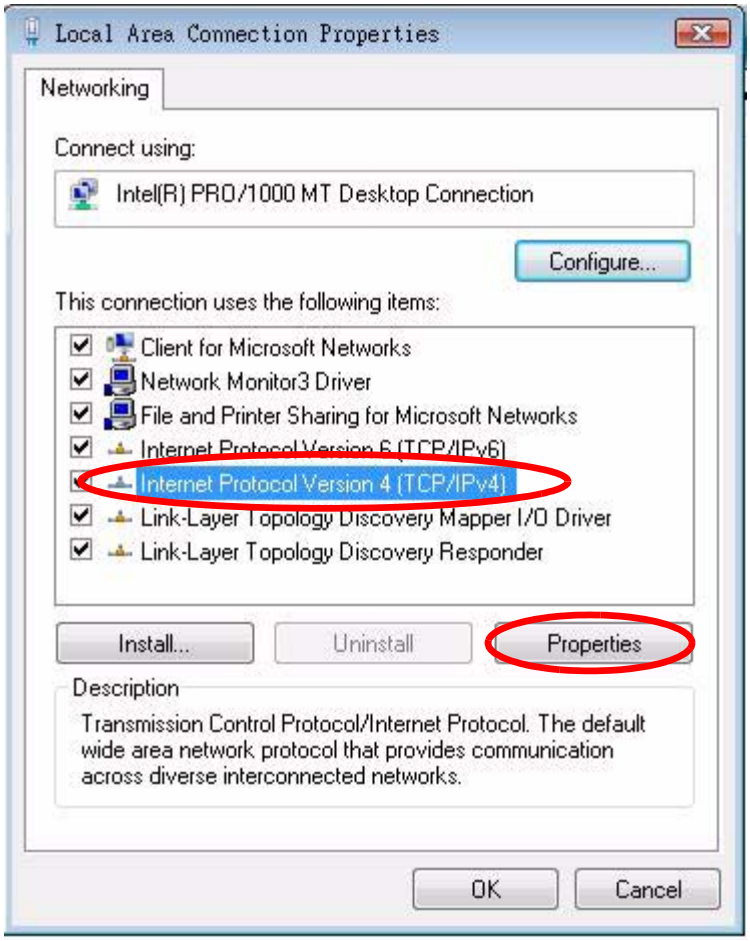
Figure 128 Windows Vista: Network and Sharing Center



Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

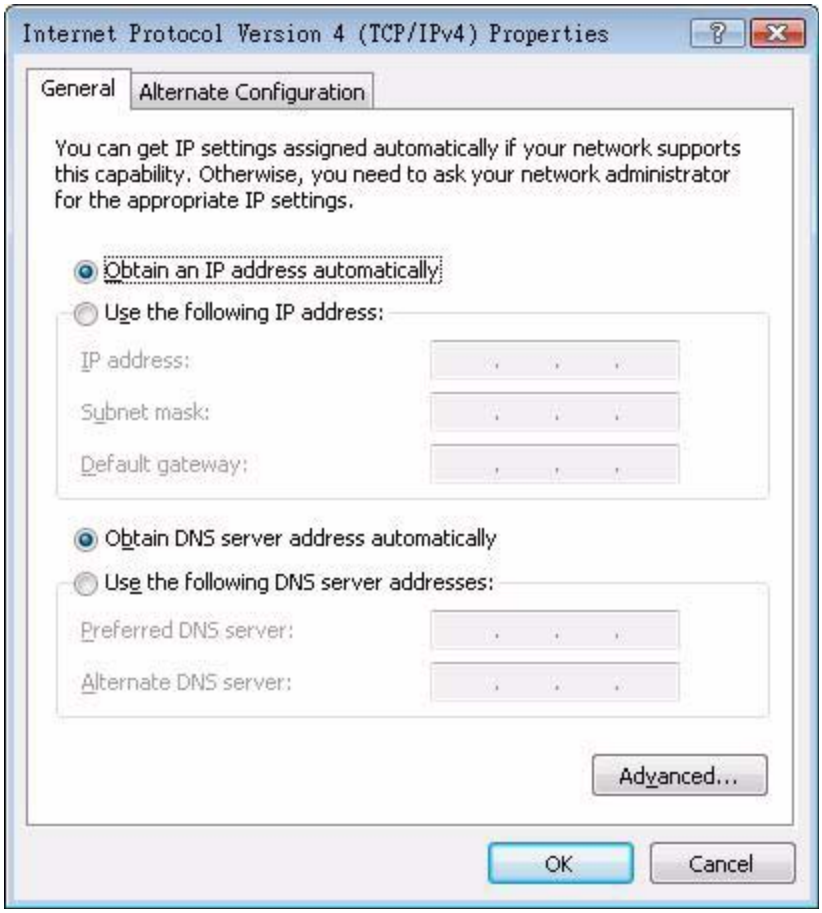
6 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.

Figure 129 Windows Vista: Local Area Connection Properties



7 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.

Figure 130 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties


Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

8 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided.Click **Advanced**.

9 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

10 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

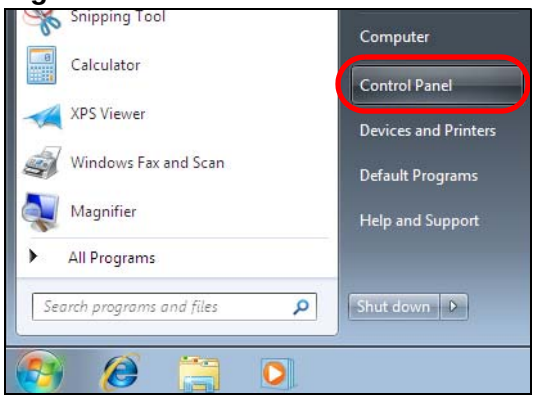
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

Windows 7

This section shows screens from Windows 7 Enterprise.

1 Click **Start** > **Control Panel**.

Figure 131 Windows 7: Start Menu

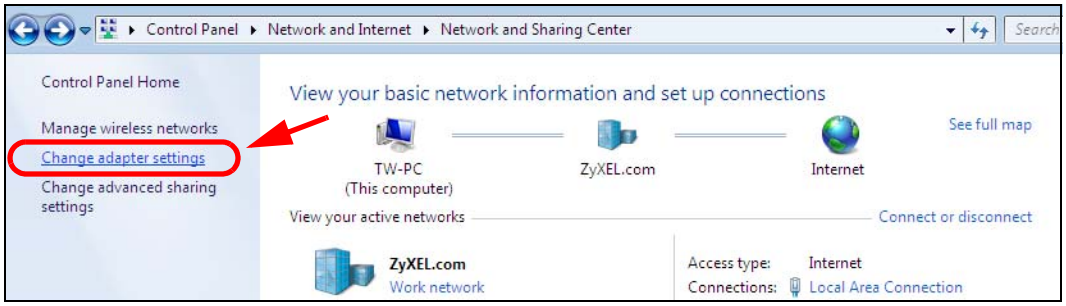


2 In the **Control Panel**, click **View network status and tasks** under the **Network and Internet** category.

Figure 132 Windows 7: Control Panel

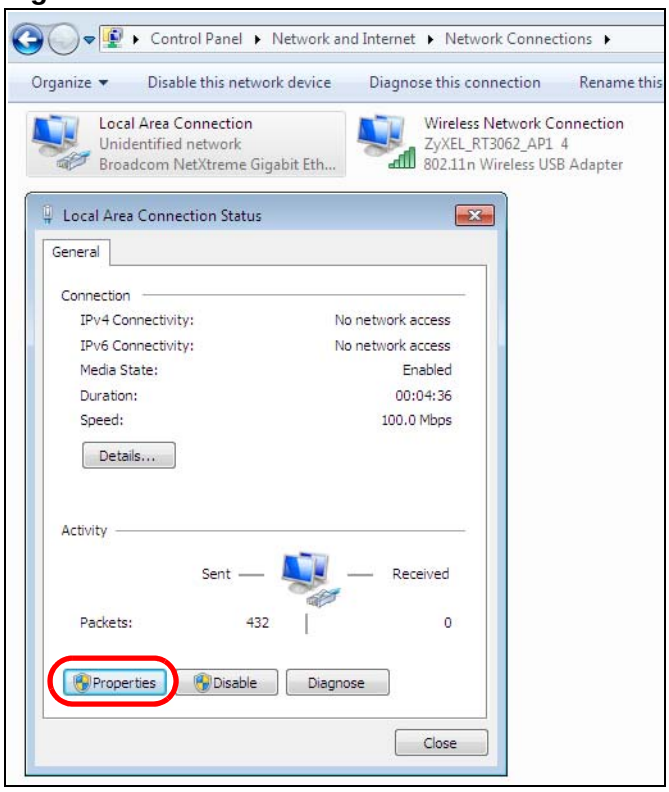
3 Click **Change adapter settings**.

Figure 133 Windows 7: Network And Sharing Center



4 Double click **Local Area Connection** and then select **Properties**.

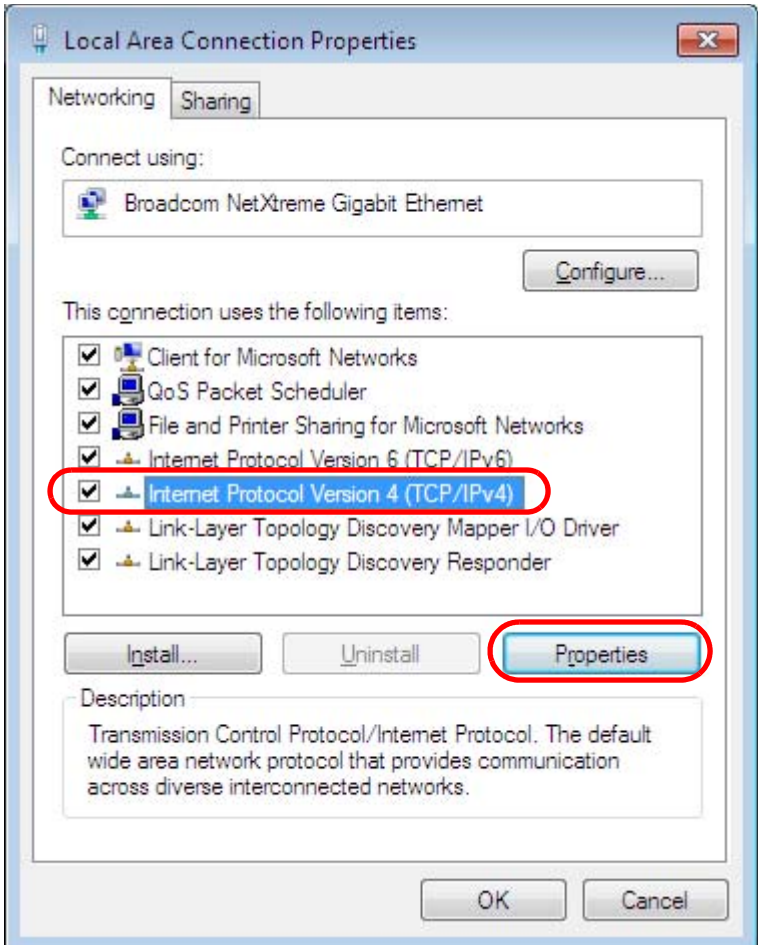
Figure 134 Windows 7: Local Area Connection Status



Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

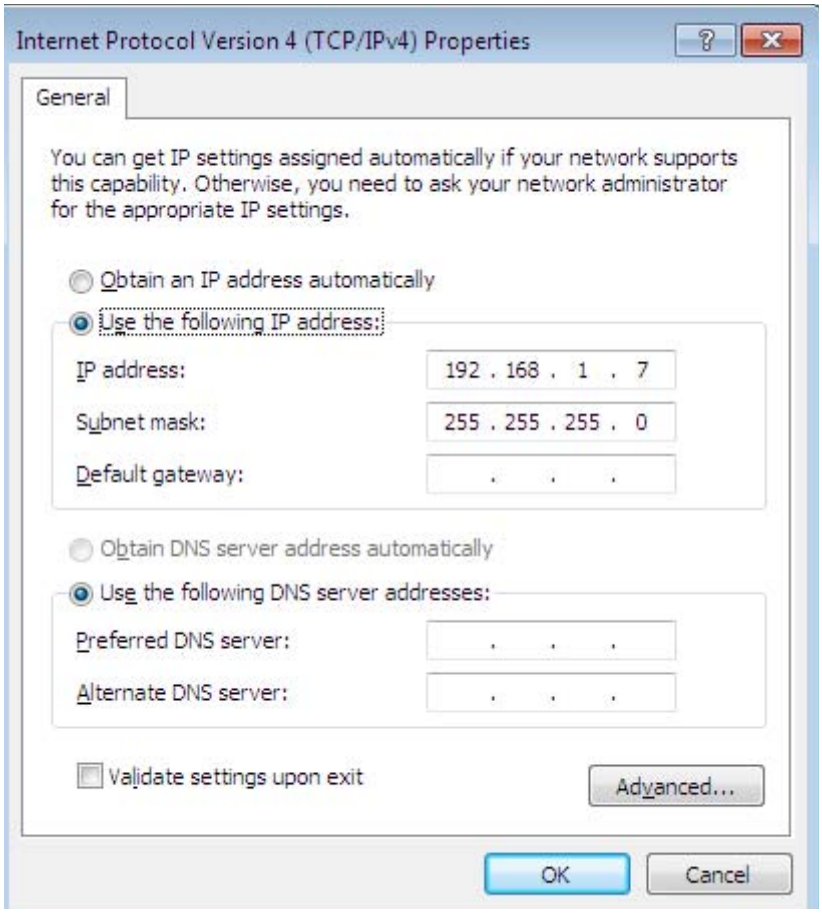
5 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.

Figure 135 Windows 7: Local Area Connection Properties



6 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.

Figure 136 Windows 7: Internet Protocol Version 4 (TCP/IPv4) Properties


Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 1 . 7
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

7 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided. Click **Advanced** if you want to configure advanced settings for IP, DNS and WINS.

8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **OK** to close the **Local Area Connection Properties** window.

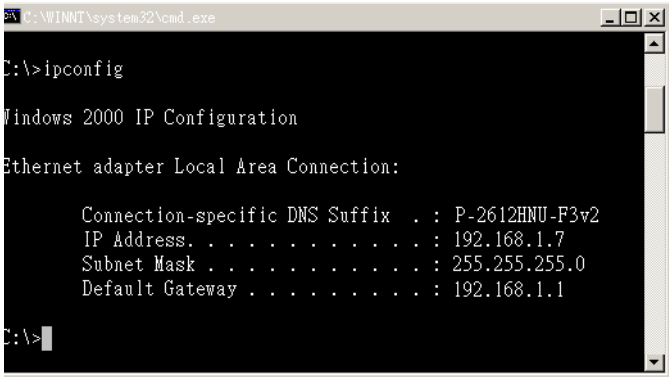
Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

3 The IP settings are displayed as follows.

Figure 137 Windows 7: Internet Protocol Version 4 (TCP/IPv4) Properties

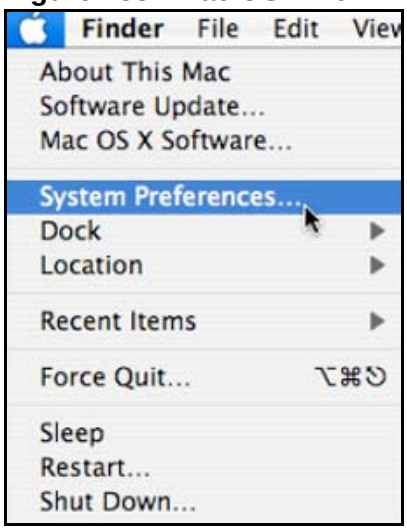

C:\WINNT\system32\cmd.exe
C:\>ipconfig
Windows 2000 IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . : P-2612HNU-F3v2
IP Address. . . . . : 192.168.1.7
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
C:\>

Mac OS X: 10.3 and 10.4

The screens in this section are from Mac OS X 10.4 but can also apply to 10.3.

1 Click **Apple** > **System Preferences**.

Figure 138 Mac OS X 10.4: Apple Menu

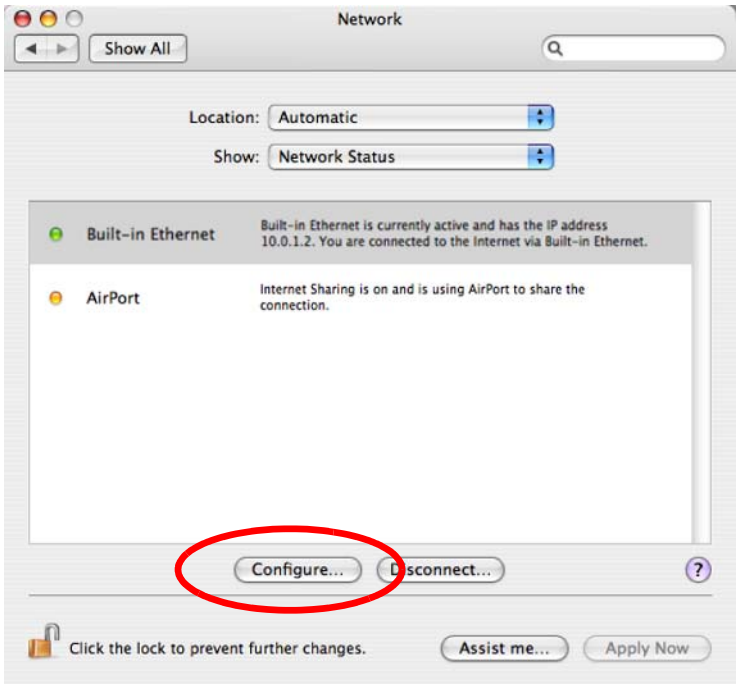


2 In the **System Preferences** window, click the **Network** icon.

Figure 139 Mac OS X 10.4: System Preferences

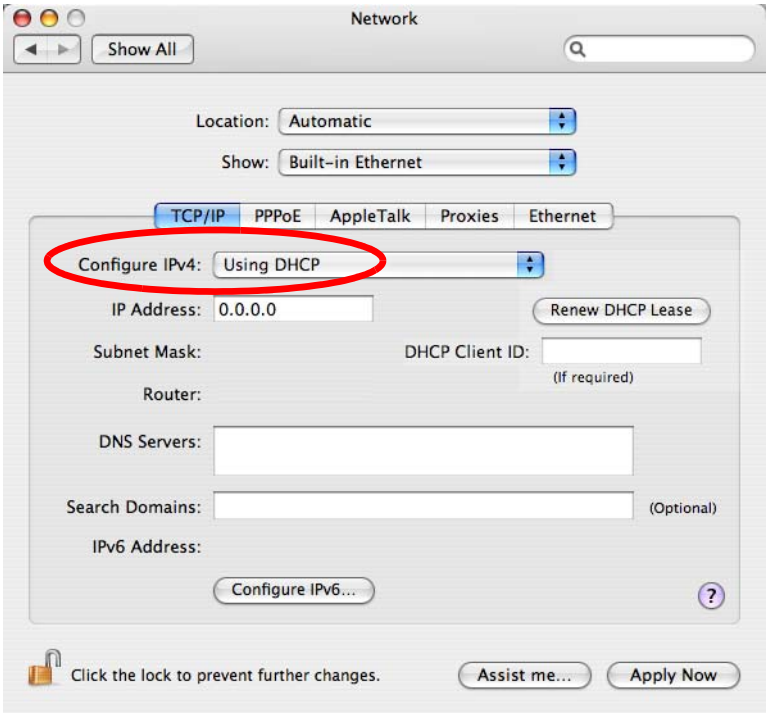
3 When the **Network** preferences pane opens, select **Built-in Ethernet** from the network connection type list, and then click **Configure.**

Figure 140 Mac OS X 10.4: Network Preferences


Network
Show All
Location: Automatic
Show: Network Status
Built-in Ethernet
Built-in Ethernet is currently active and has the IP address 10.0.1.2. You are connected to the Internet via Built-in Ethernet.
AirPort
Internet Sharing is on and is using AirPort to share the connection.
Configure...
Disconnect...
Click the lock to prevent further changes.
Assist me...
Apply Now

4 For dynamically assigned settings, select **Using DHCP** from the **Configure IPv4** list in the **TCP/IP** tab.

Figure 141 Mac OS X 10.4: Network Preferences > TCP/IP Tab.

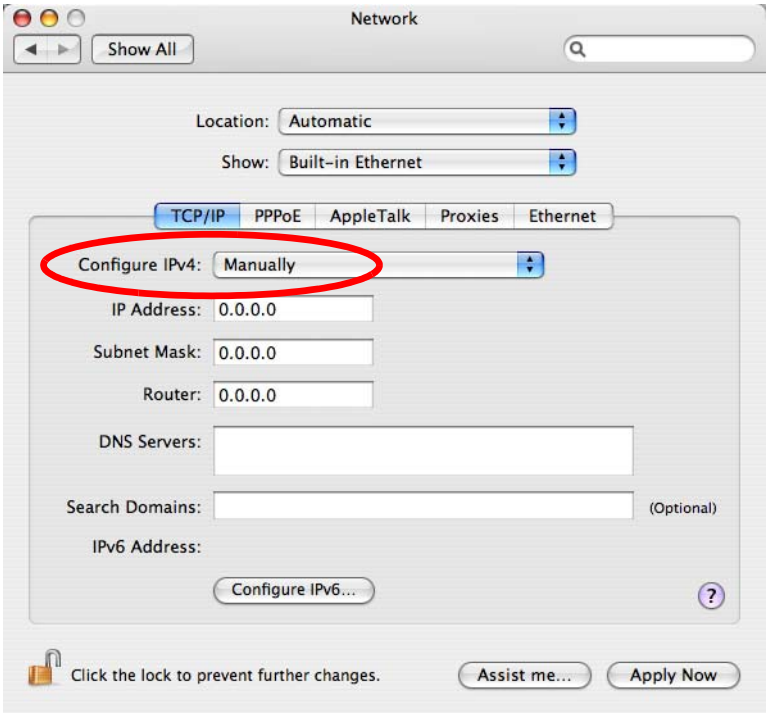


5 For statically assigned settings, do the following:

- From the **Configure IPv4** list, select **Manually**.
- In the **IP Address** field, type your IP address.
- In the **Subnet Mask** field, type your subnet mask.

- In the **Router** field, type the IP address of your device.

Figure 142 Mac OS X 10.4: Network Preferences > Ethernet

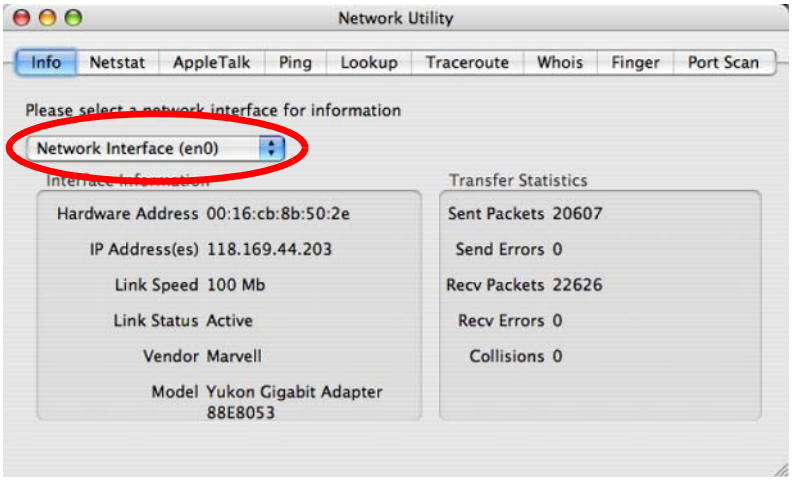


6 Click **Apply Now** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network Interface** from the **Info** tab.

Figure 143 Mac OS X 10.4: Network Utility

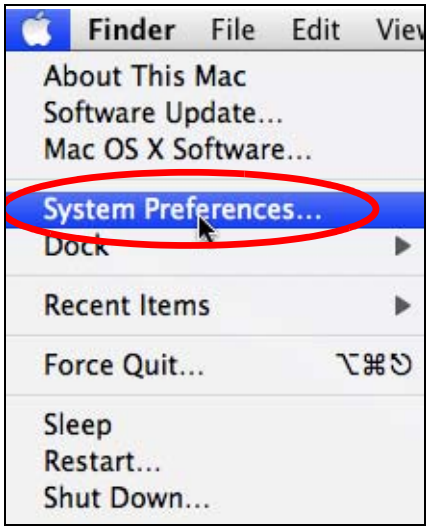


Mac OS X: 10.5

The screens in this section are from Mac OS X 10.5.

1 Click **Apple** > **System Preferences**.

Figure 144 Mac OS X 10.5: Apple Menu

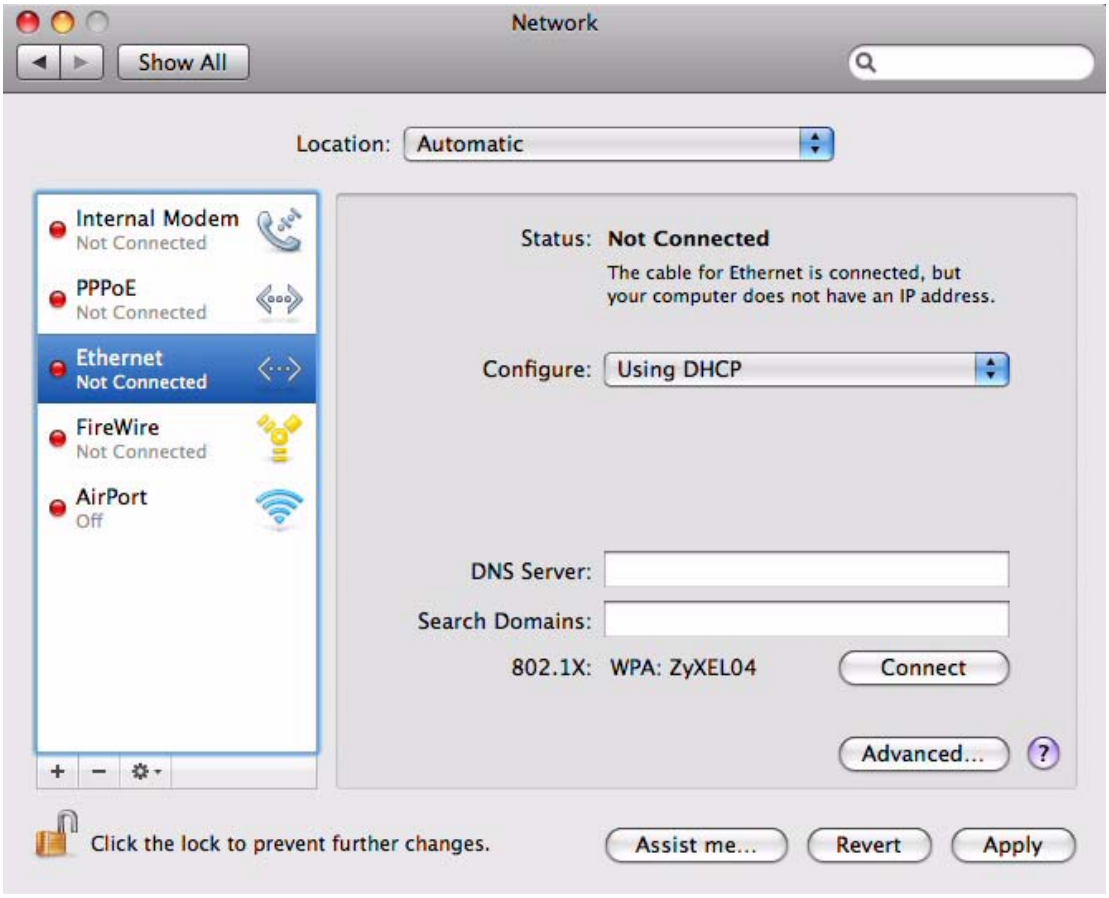


2 In **System Preferences**, click the **Network** icon.

Figure 145 Mac OS X 10.5: Systems Preferences

3 When the **Network** preferences pane opens, select **Ethernet** from the list of available connection types.

Figure 146 Mac OS X 10.5: Network Preferences > Ethernet



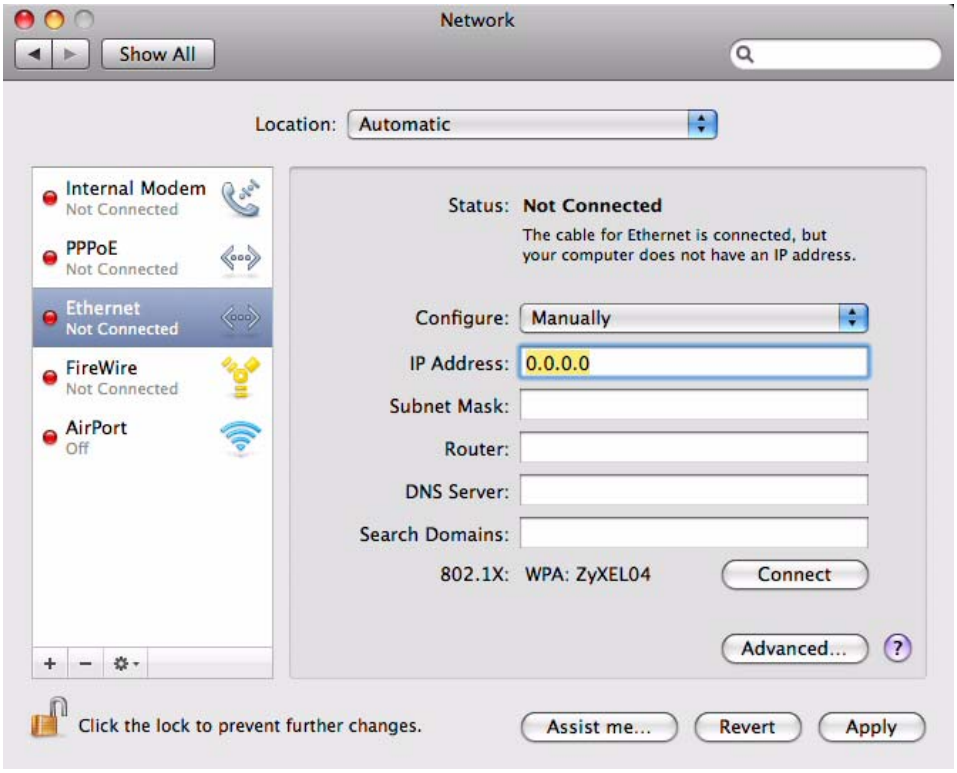
4 From the **Configure** list, select **Using DHCP** for dynamically assigned settings.

5 For statically assigned settings, do the following:

- From the **Configure** list, select **Manually**.
- In the **IP Address** field, enter your IP address.
- In the **Subnet Mask** field, enter your subnet mask.

- In the **Router** field, enter the IP address of your ZyXEL Device.

Figure 147 Mac OS X 10.5: Network Preferences > Ethernet

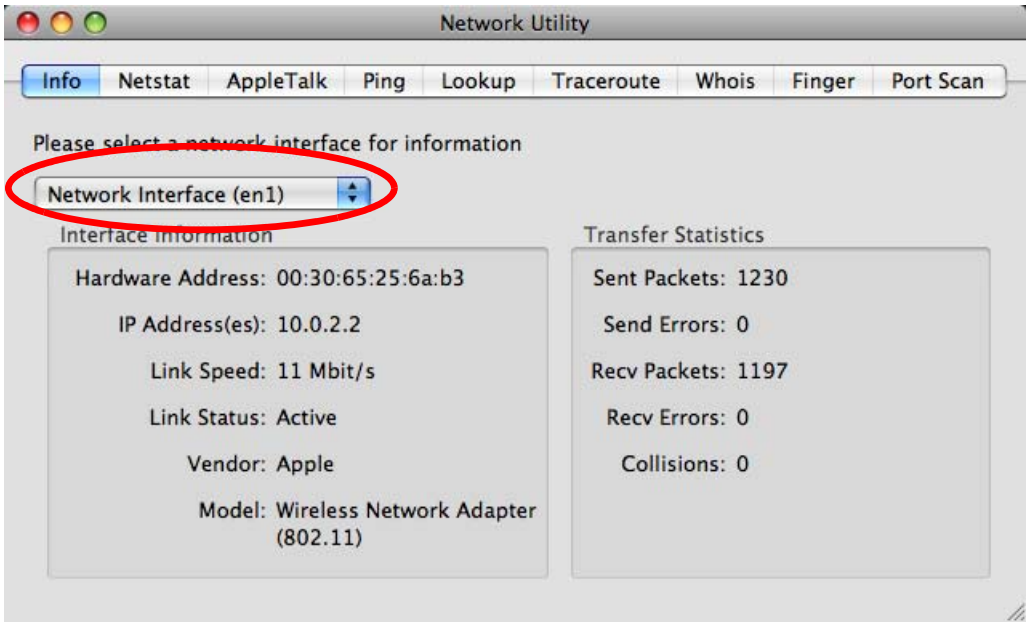


6 Click **Apply** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network interface** from the **Info** tab.

Figure 148 Mac OS X 10.5: Network Utility



Linux: Ubuntu 8 (GNOME)

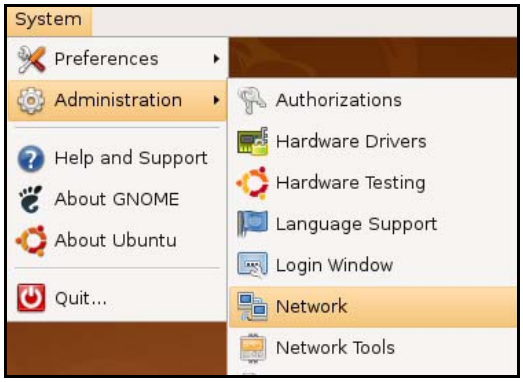
This section shows you how to configure your computer's TCP/IP settings in the GNU Object Model Environment (GNOME) using the Ubuntu 8 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default Ubuntu 8 installation.

Note: Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in GNOME:

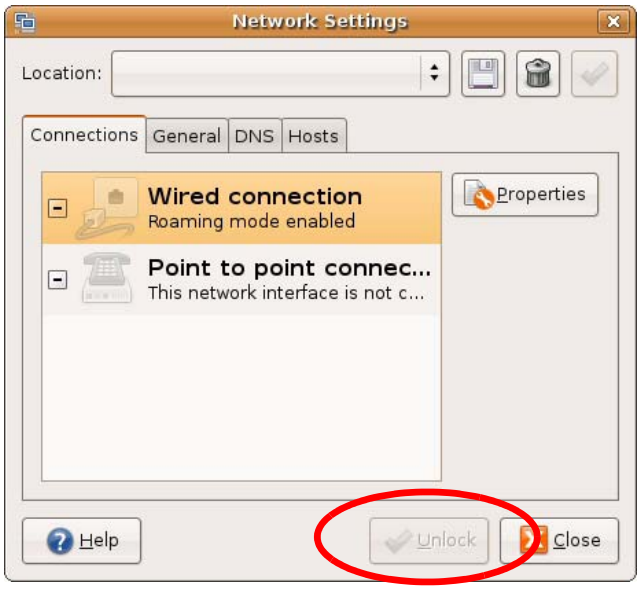
1 Click **System > Administration > Network**.

Figure 149 Ubuntu 8: System > Administration Menu



2 When the **Network Settings** window opens, click **Unlock** to open the **Authenticate** window. (By default, the **Unlock** button is greyed out until clicked.) You cannot make changes to your configuration unless you first enter your admin password.

Figure 150 Ubuntu 8: Network Settings > Connections



3 In the **Authenticate** window, enter your admin account name and password then click the **Authenticate** button.

Figure 151 Ubuntu 8: Administrator Account Authentication

Authenticate
System policy prevents modifying the configuration
An application is attempting to perform an action that requires privileges. Authentication as one of the users below is required to perform this action.
C.J.,,,, (chris)
Password for chris:
Details
Cancel
Authenticate

4 In the **Network Settings** window, select the connection that you want to configure, then click **Properties**.

Figure 152 Ubuntu 8: Network Settings > Connections

5 The **Properties** dialog box opens.

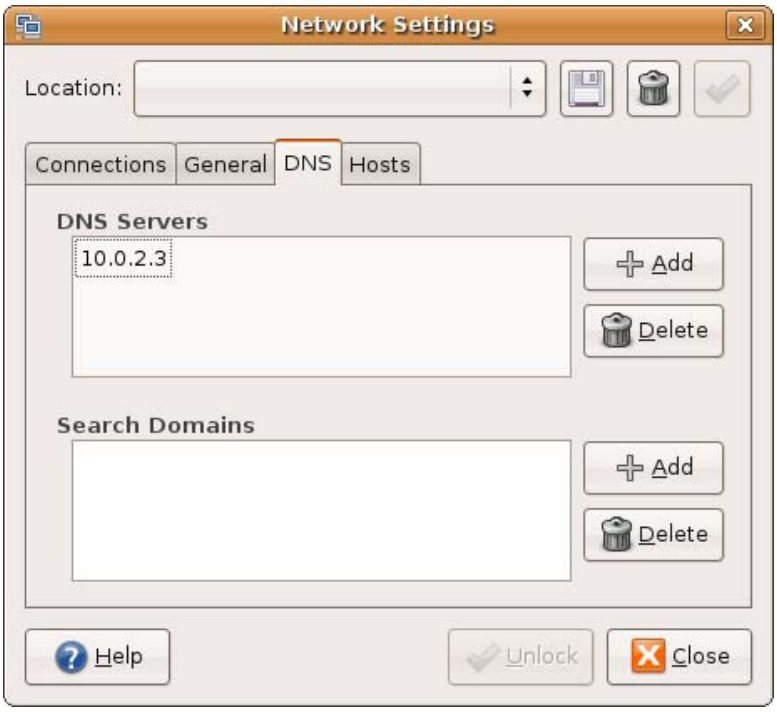
Figure 153 Ubuntu 8: Network Settings > Properties

- In the **Configuration** list, select **Automatic Configuration (DHCP)** if you have a dynamic IP address.
- In the **Configuration** list, select **Static IP address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Gateway address** fields.

6 Click **OK** to save the changes and close the **Properties** dialog box and return to the **Network Settings** screen.

7 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Settings** window and then enter the DNS server information in the fields provided.

Figure 154 Ubuntu 8: Network Settings > DNS



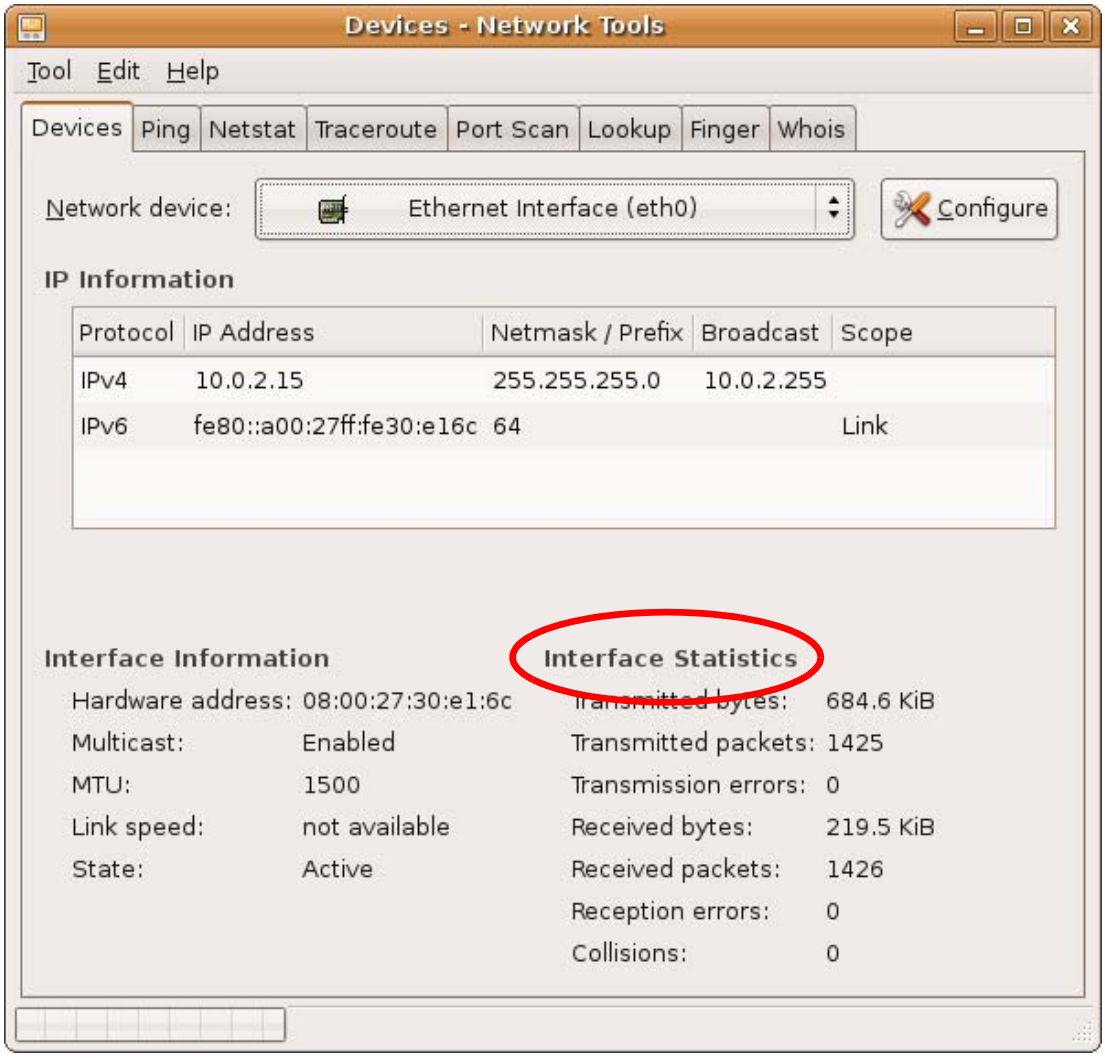
8 Click the **Close** button to apply the changes.

Verifying Settings

Check your TCP/IP properties by clicking **System > Administration > Network Tools**, and then selecting the appropriate **Network device** from the **Devices**

tab. The **Interface Statistics** column shows data if your connection is working properly.

Figure 155 Ubuntu 8: Network Tools



Linux: openSUSE 10.3 (KDE)

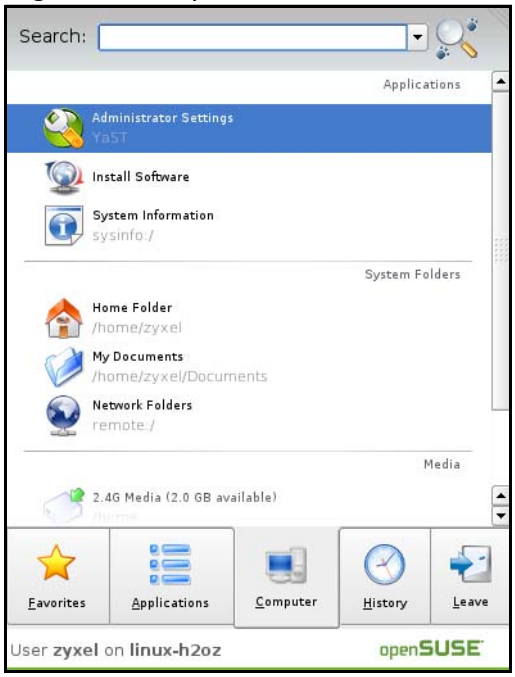
This section shows you how to configure your computer's TCP/IP settings in the K Desktop Environment (KDE) using the openSUSE 10.3 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default openSUSE 10.3 installation.

Note: Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in the KDE:

1 Click **K Menu > Computer > Administrator Settings (YaST)**.

Figure 156 openSUSE 10.3: K Menu > Computer Menu

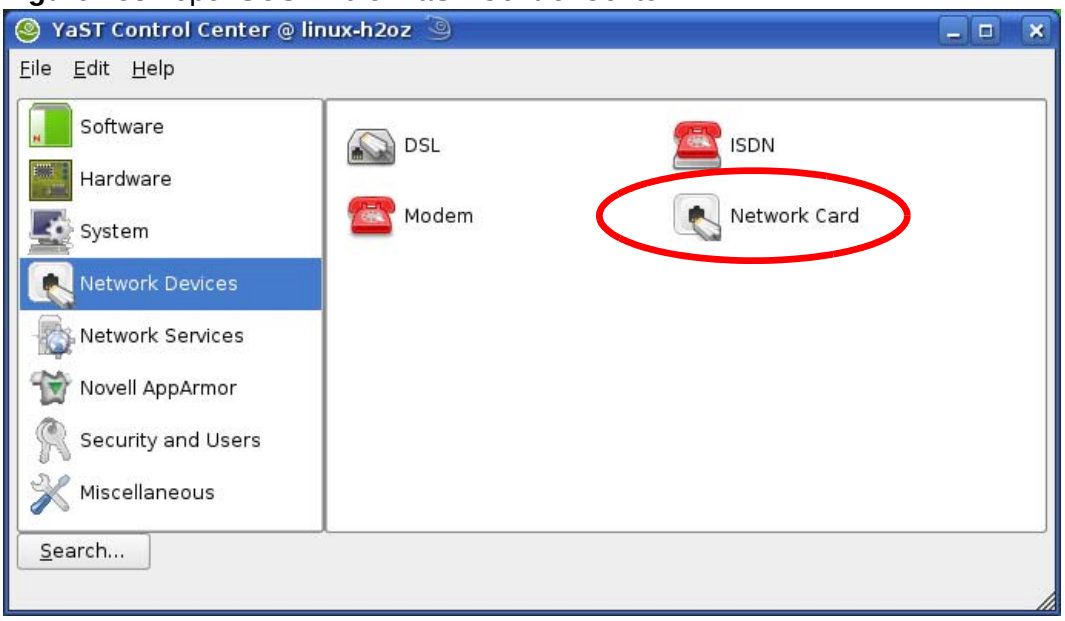


2 When the **Run as Root - KDE su** dialog opens, enter the admin password and click **OK**.

Figure 157 openSUSE 10.3: K Menu > Computer Menu

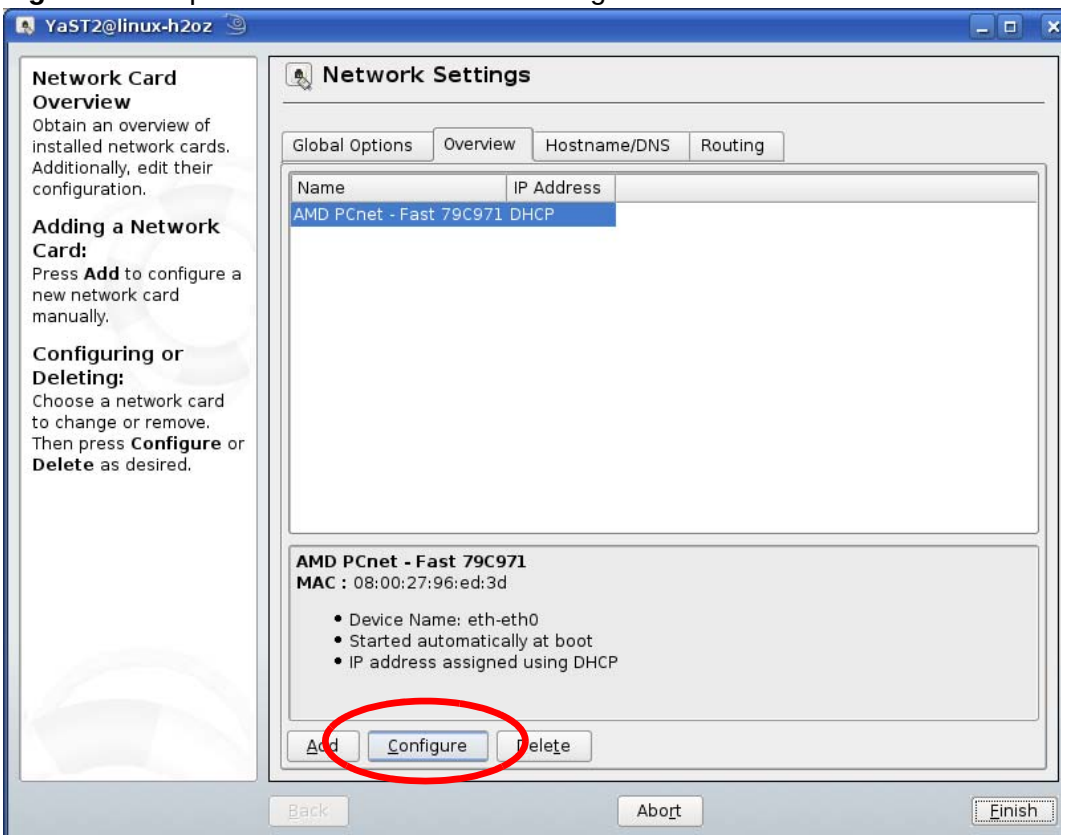
3 When the **YaST Control Center** window opens, select **Network Devices** and then click the **Network Card** icon.

Figure 158 openSUSE 10.3: YaST Control Center



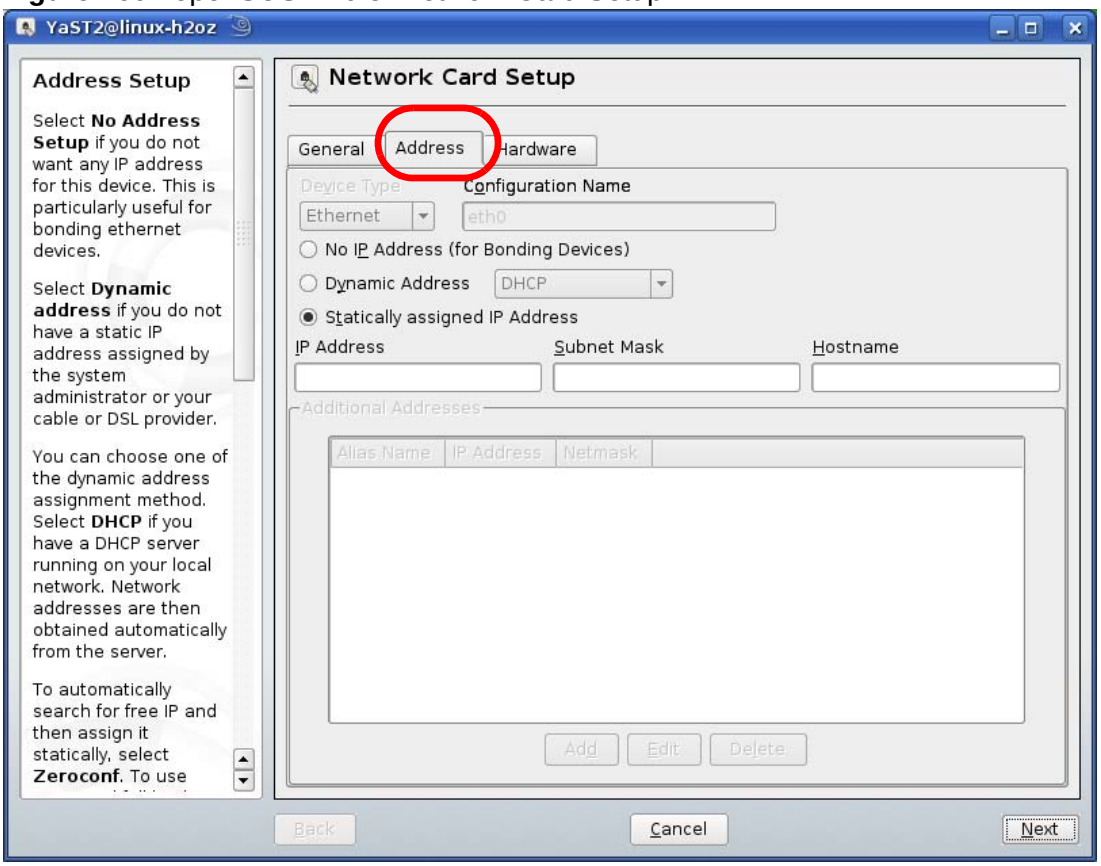
4 When the **Network Settings** window opens, click the **Overview** tab, select the appropriate connection **Name** from the list, and then click the **Configure** button.

Figure 159 openSUSE 10.3: Network Settings



5 When the **Network Card Setup** window opens, click the **Address** tab

Figure 160 openSUSE 10.3: Network Card Setup


YaST2@linux-h2oz
Address Setup
Select No Address Setup if you do not want any IP address for this device. This is particularly useful for bonding ethernet devices.
Select Dynamic address if you do not have a static IP address assigned by the system administrator or your cable or DSL provider.
You can choose one of the dynamic address assignment method. Select DHCP if you have a DHCP server running on your local network. Network addresses are then obtained automatically from the server.
To automatically search for free IP and then assign it statically, select Zeroconf. To use
Network Card Setup
General
Address
Hardware
Device Type
Configuration Name
Ethernet
eth0
No IP Address (for Bonding Devices)
Dynamic Address
DHCP
Statically assigned IP Address
IP Address
Subnet Mask
Hostname
Additional Addresses
Alias Name
IP Address
Netmask
Add
Edit
Delete
Back
Cancel
Next

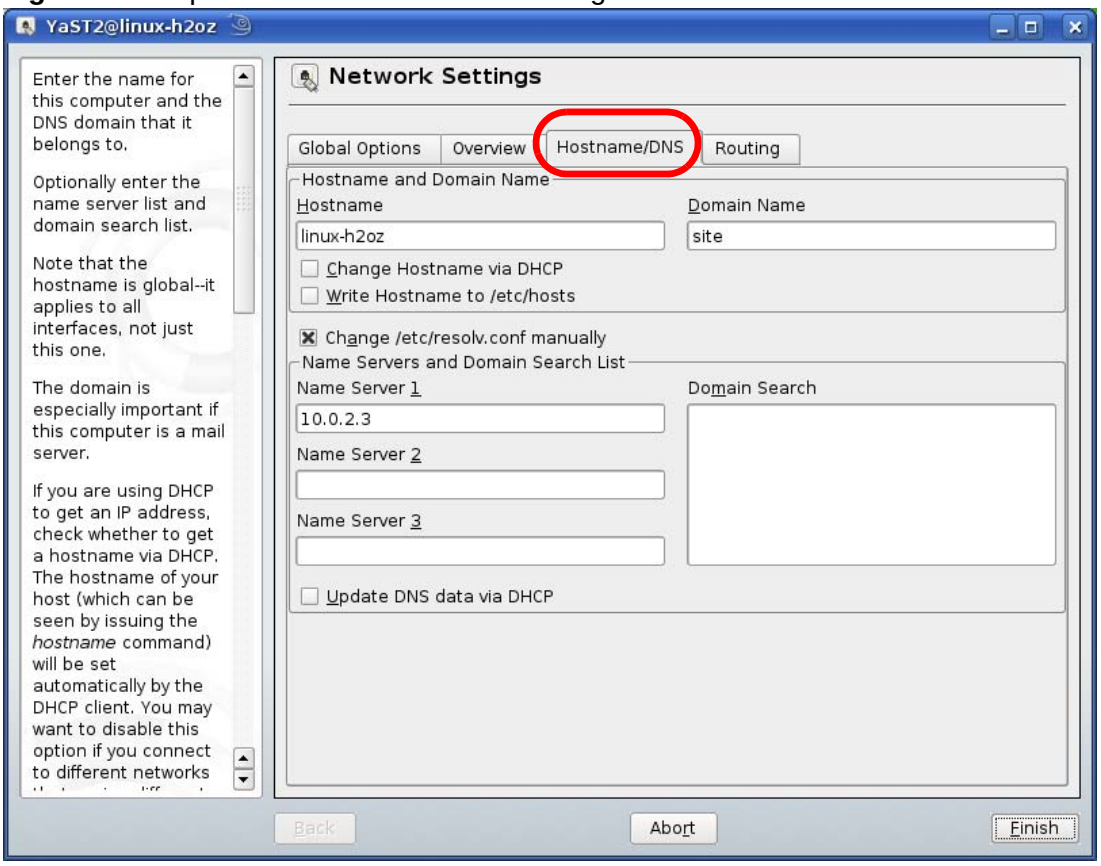
6 Select **Dynamic Address (DHCP)** if you have a dynamic IP address.

Select **Statically assigned IP Address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Hostname** fields.

7 Click **Next** to save the changes and close the **Network Card Setup** window.

8 If you know your DNS server IP address(es), click the **Hostname/DNS** tab in **Network Settings** and then enter the DNS server information in the fields provided.

Figure 161 openSUSE 10.3: Network Settings


YaST2@linux-h2oz
Enter the name for this computer and the DNS domain that it belongs to.
Optionally enter the name server list and domain search list.
Note that the hostname is global--it applies to all interfaces, not just this one.
The domain is especially important if this computer is a mail server.
If you are using DHCP to get an IP address, check whether to get a hostname via DHCP. The hostname of your host (which can be seen by issuing the hostname command) will be set automatically by the DHCP client. You may want to disable this option if you connect to different networks
Network Settings
Global Options
Overview
Hostname/DNS
Routing
Hostname and Domain Name
Hostname
linux-h2oz
Domain Name
site
Change Hostname via DHCP
Write Hostname to /etc/hosts
Change /etc/resolv.conf manually
Name Servers and Domain Search List
Name Server 1
10.0.2.3
Domain Search
Name Server 2
Name Server 3
Update DNS data via DHCP
Back
Abort
Finish

9 Click **Finish** to save your settings and close the window.

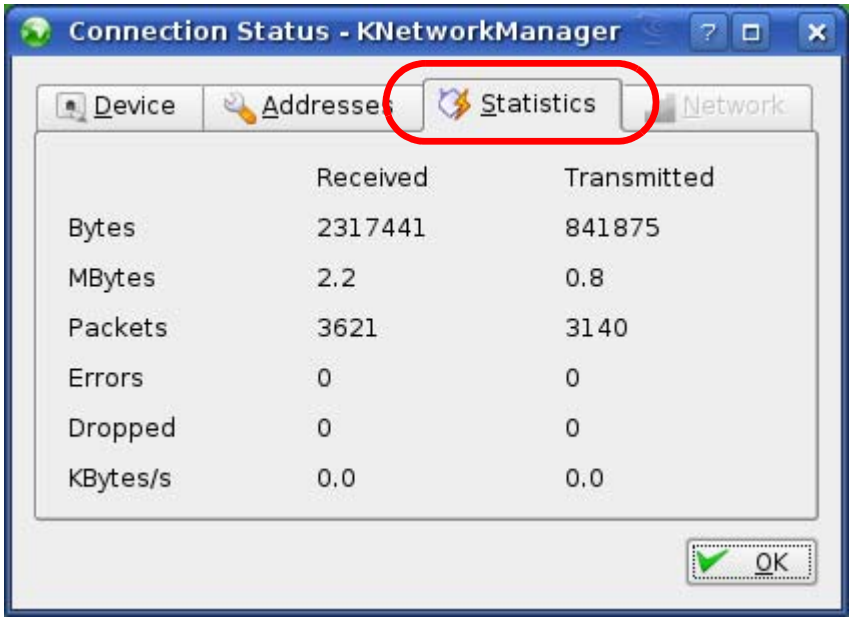
Verifying Settings

Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

Figure 162 openSUSE 10.3: KNetwork Manager

When the **Connection Status - KNetwork Manager** window opens, click the **Statistics tab** to see if your connection is working properly.

Figure 163 openSUSE: Connection Status - KNetwork Manager



C

Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Note: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

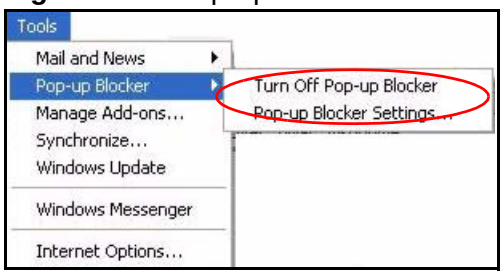
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

Disable Pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 164 Pop-up Blocker



You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 165 Internet Options: Privacy

3 Click **Apply** to save this setting.

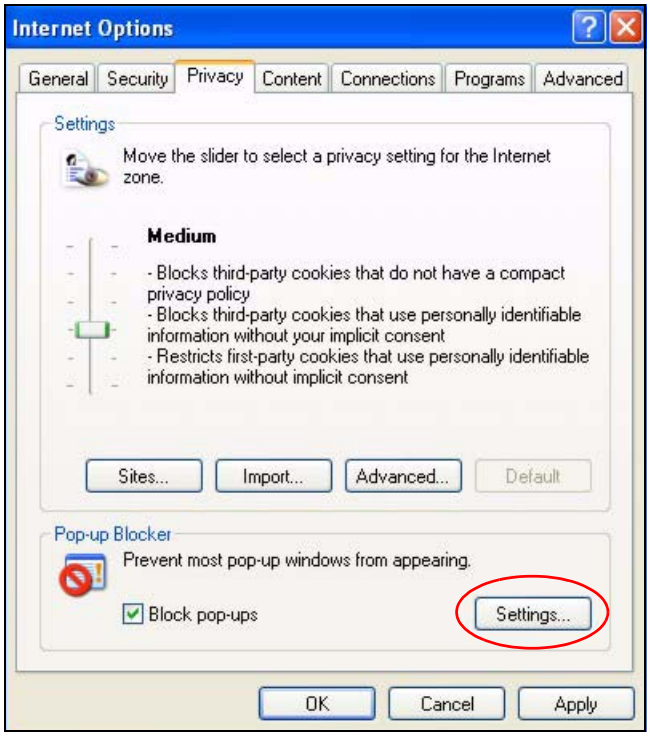
Enable Pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings...**to open the **Pop-up Blocker Settings** screen.

Figure 166 Internet Options: Privacy



3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix “http://”. For example, http://192.168.167.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 167 Pop-up Blocker Settings

Pop-up Blocker Settings
Exceptions
Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.
Address of Web site to allow:
http://192.168.1.1
Add
Allowed sites:
Remove
Remove All
Notifications and Filter Level
Play a sound when a pop-up is blocked.
Show Information Bar when a pop-up is blocked.
Filter Level:
Medium: Block most automatic pop-ups
Pop-up Blocker FAQ
Close

5 Click **Close** to return to the **Privacy** screen.

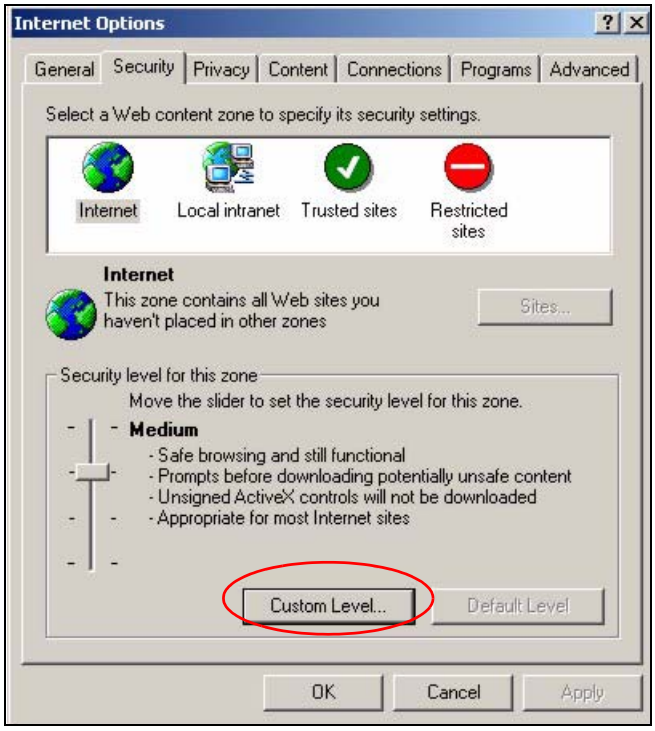
6 Click **Apply** to save this setting.

JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 168 Internet Options: Security



2 Click the **Custom Level...** button.

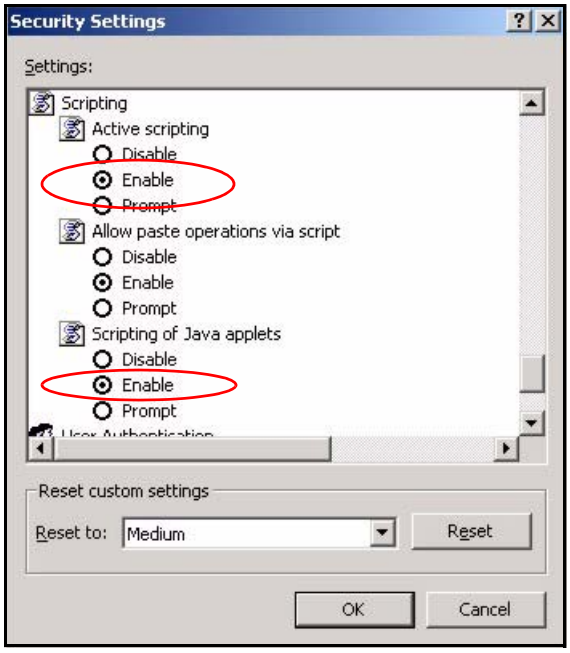
3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

Figure 169 Security Settings - Java Scripting



Java Permissions

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

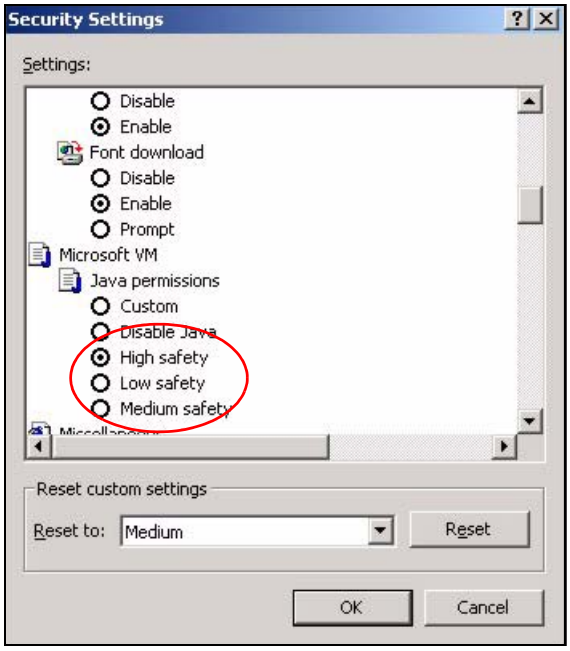
2 Click the **Custom Level...** button.

3 Scroll down to **Microsoft VM**.

4 Under **Java permissions** make sure that a safety level is selected.

5 Click **OK** to close the window.

Figure 170 Security Settings - Java



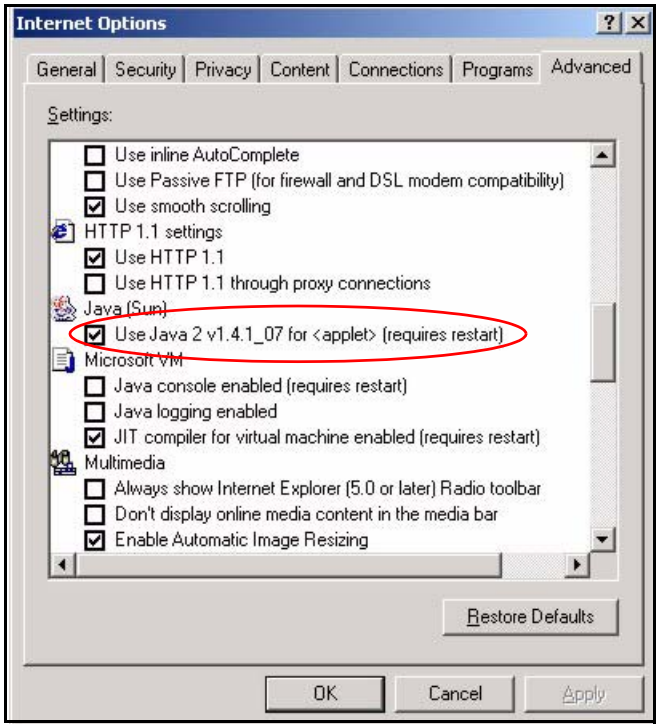
JAVA (Sun)

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.

2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

3 Click **OK** to close the window.

Figure 171 Java (Sun)

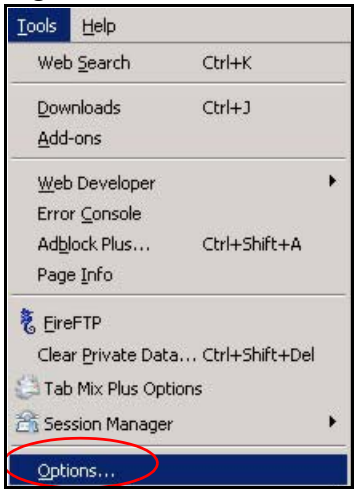


Mozilla Firefox

Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary.

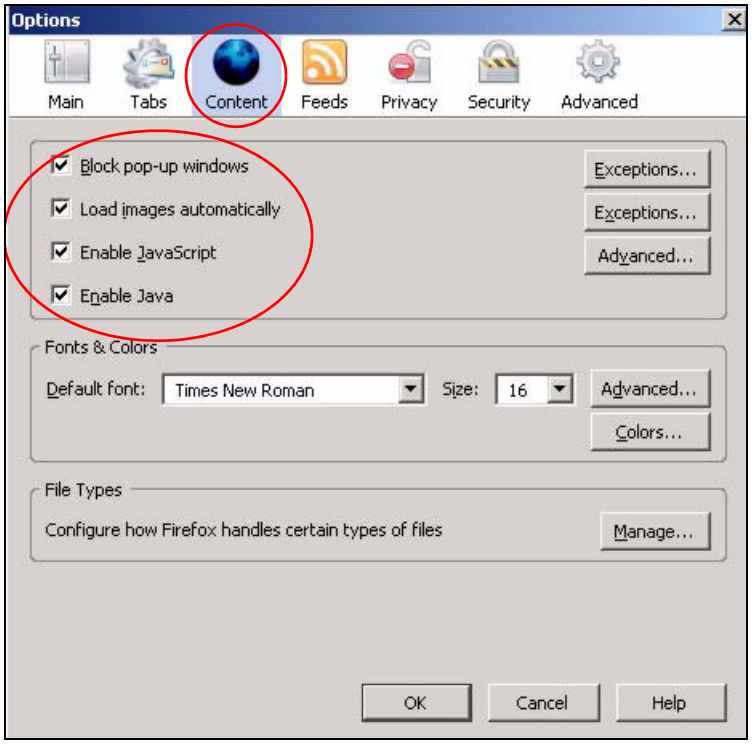
You can enable Java, Javascripts and pop-ups in one screen. Click **Tools,** then click **Options** in the screen that appears.

Figure 172 Mozilla Firefox: Tools > Options



Click **Content**.to show the screen below. Select the check boxes as shown in the following screen.

Figure 173 Mozilla Firefox Content Security



D

Wireless LANs

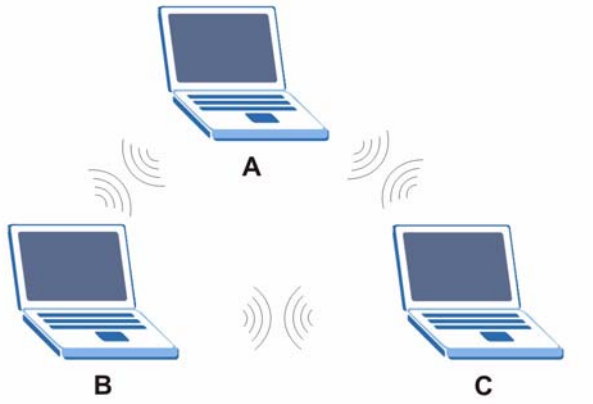
Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless adapters (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an ad-hoc wireless LAN.

Figure 174 Peer-to-Peer Communication in an Ad-hoc Network



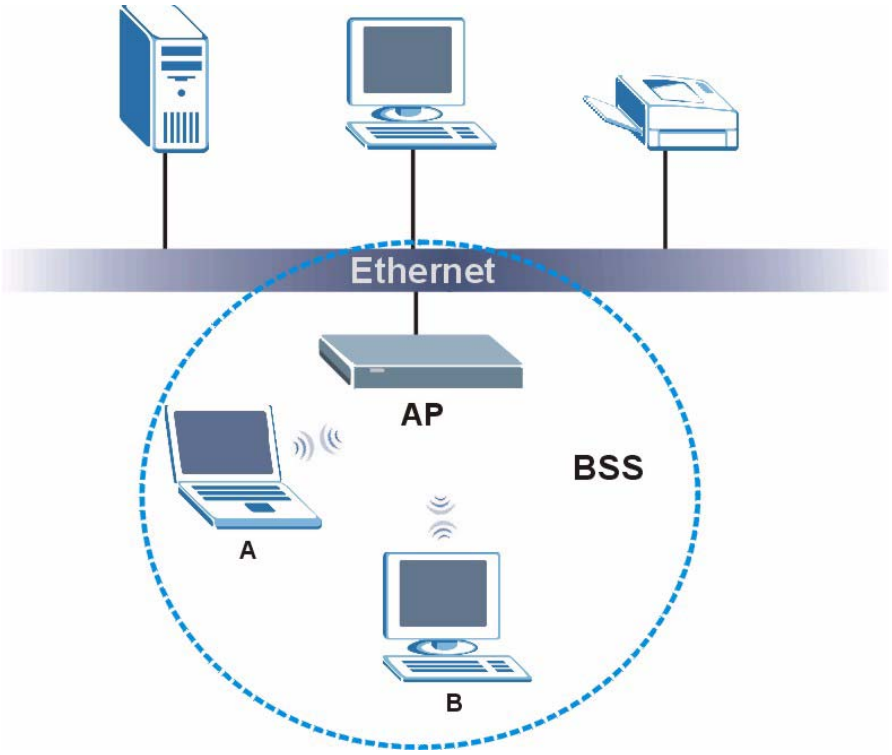
BSS

A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client **A** and **B** can access the wired network and communicate

with each other. When Intra-BSS is disabled, wireless client **A** and **B** can still access the wired network but cannot communicate with each other.

Figure 175 Basic Service Set



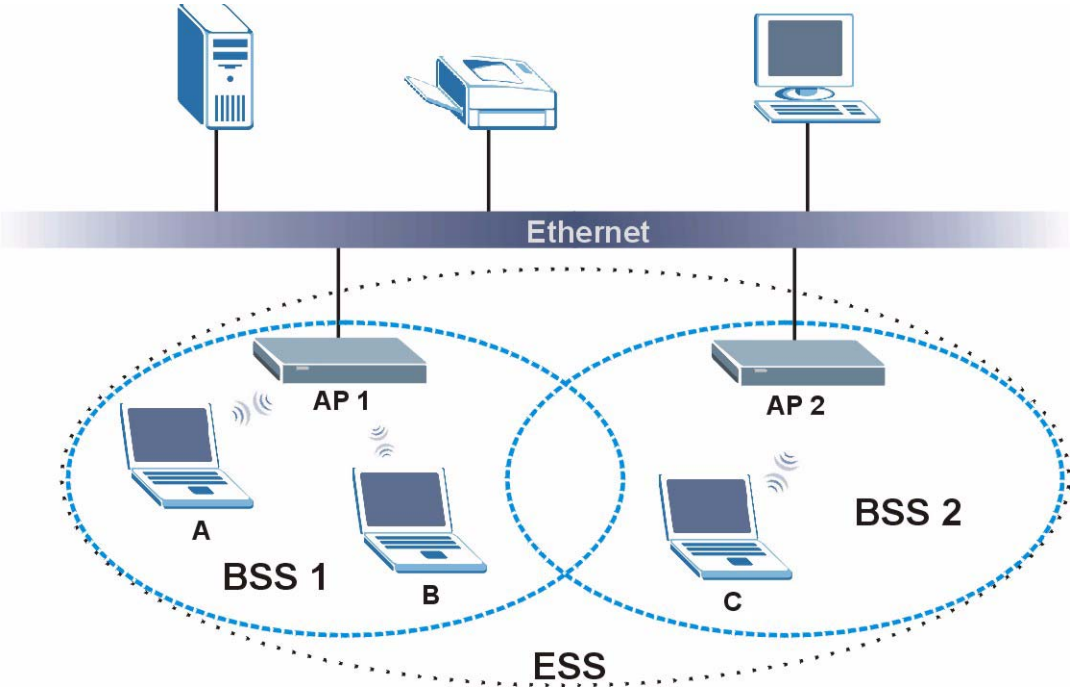
ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless clients within the same ESS must have the same ESSID in order to communicate.

Figure 176 Infrastructure WLAN



Channel

A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

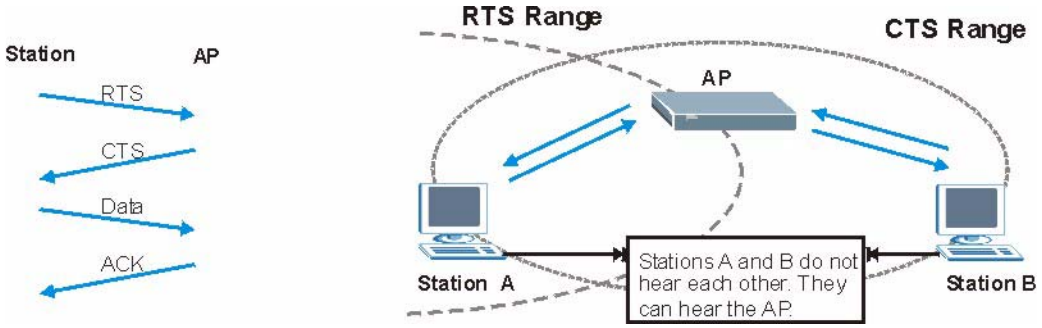
Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or

wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 177 RTS/CTS



When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Preamble Type

Preamble is used to signal that data is coming to the receiver. Short and long refer to the length of the synchronization field in a packet.

Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11 compliant wireless adapters support long preamble, but not all support short preamble.

Use long preamble if you are unsure what preamble mode other wireless devices on the network support, and to provide more reliable communications in busy wireless networks.

Use short preamble if you are sure all wireless devices on the network support it, and to provide more efficient communications.

Use the dynamic setting to automatically use short preamble when all wireless devices on the network support it, otherwise the ZyXEL Device uses long preamble.

Note: The wireless devices MUST use the same preamble mode in order to communicate.

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has

several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 101 IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/ 48/54	OFDM (Orthogonal Frequency Division Multiplexing)

Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between wireless clients, access points and the wired network.

Wireless security methods available on the ZyXEL Device are data encryption, wireless client authentication, restricting access by device MAC address and hiding the ZyXEL Device identity.

The following figure shows the relative effectiveness of these wireless security methods available on your ZyXEL Device.

Table 102 Wireless Security Levels

SECURITY LEVEL	SECURITY TYPE
Least Secure	Unique SSID (Default)
	Unique SSID with Hide SSID Enabled
	MAC Address Filtering
	WEP Encryption
	IEEE802.1x EAP with RADIUS Server Authentication
	Wi-Fi Protected Access (WPA)
Most Secure	WPA2

Note: You must enable the same wireless security settings on the ZyXEL Device and on all wireless clients that you want to associate with it.

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless clients.

RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication

  Determines the identity of the users.
- Authorization

  Determines the network services available to authenticated users once they are connected to the network.
- Accounting

  Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless client and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request

  Sent by an access point requesting authentication.
- Access-Reject

  Sent by a RADIUS server rejecting access.
- Access-Accept

  Sent by a RADIUS server allowing access.

- Access-Challenge

  Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request

  Sent by the access point requesting accounting.

- Accounting-Response

  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x. .

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless client. The wireless client ‘proves’ that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the wireless security configuration screen. You may still configure and store keys, but they will not be used while dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 103 Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA or WPA2 and WEP are improved data encryption and user authentication.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

Encryption

Both WPA and WPA2 improve data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA and WPA2 use Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption than TKIP.

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a Wi-Fi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption

keys. This prevent all wireless devices sharing the same encryption keys. (a weakness of WEP)

User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a wireless client to store the PMK it derived through a successful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

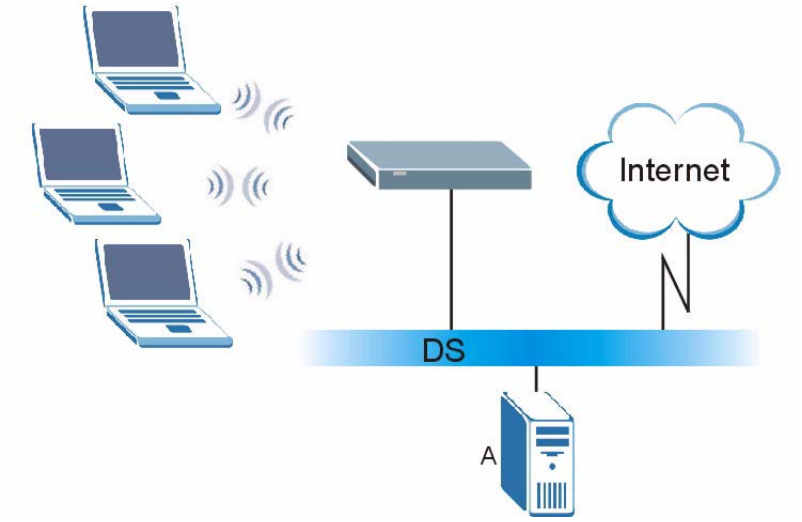
WPA(2) with RADIUS Application Example

To set up WPA(2), you need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

1. The AP passes the wireless client's authentication request to the RADIUS server.
2. The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
3. A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.

4 The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 178 WPA(2) with RADIUS Application Example



WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

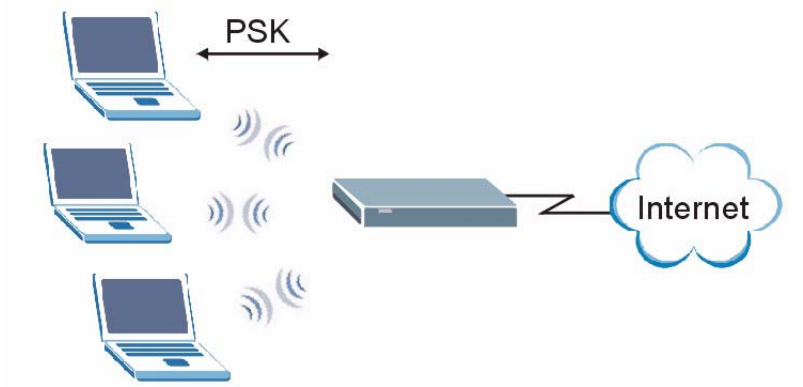
1 First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).

2 The AP checks each wireless client's password and allows it to join the network only if the password matches.

3 The AP and wireless clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.

4 The AP and wireless clients use the TKIP or AES encryption process, the PMK and information exchanged in a handshake to create temporal encryption keys. They use these keys to encrypt data exchanged between them.

Figure 179 WPA(2)-PSK Authentication



Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each authentication method or key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 104 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP/AES	No	Enable
WPA-PSK	TKIP/AES	Yes	Disable
WPA2	TKIP/AES	No	Enable
WPA2-PSK	TKIP/AES	Yes	Disable

Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b and IEEE 802.11g) or 5GHz (IEEE 802.11a) is needed to communicate efficiently in a wireless LAN

Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Types of Antennas for WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to–point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

WiFi Protected Setup

Your ZyXEL Device supports WiFi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the WiFi Alliance.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Each WPS connection works between two devices. Both devices must support WPS (check each device's documentation to make sure).

Depending on the devices you have, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (a unique Personal Identification Number that allows one device to authenticate the other) in each of the two devices. When WPS is activated on a device, it has two minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

Push Button Configuration

WPS Push Button Configuration (PBC) is initiated by pressing a button on each WPS-enabled device, and allowing them to connect automatically. You do not need to enter any information.

Not every WPS-enabled device has a physical WPS button. Some may have a WPS PBC button in their configuration utilities instead of or in addition to the physical button.

Take the following steps to set up WPS using the button.

1. Ensure that the two devices you want to set up are within wireless range of one another.
2. Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this - for the ZyXEL Device, see Section 7.5 on page 143).
3. Press the button on one of the devices (it doesn't matter which).
4. Within two minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through an secure connection to the enrollee.

   If you need to make sure that WPS worked, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

PIN Configuration

Each WPS-enabled device has its own PIN (Personal Identification Number). This may either be static (it cannot be changed) or dynamic (you can change it to a new random number by clicking on a button in the configuration interface).

When you use the PIN method, you must enter the enrollee's PIN into the registrar. Then, when WPS is activated on the enrollee, it presents its PIN to the registrar. If the PIN matches, the registrar sends the network and security information to the enrollee, allowing it to join the network.

The advantage of using the PIN method rather than the PBC method is that you can ensure that the connection is established between the devices you specify, not just the first two devices to activate WPS in the area. However, you need to log into the configuration interfaces of both devices.

Take the following steps to set up WPS using the PIN method.

1 Decide which device you want to be the registrar (usually the AP) and which you want to be the enrollee (usually the client).

2 Look for the enrollee's WPS PIN; it may be displayed on the device. If you don't see it, log into the enrollee's configuration interface and locate the PIN. Select the PIN connection mode (not PBC connection mode). See the device's User's Guide for how to do this - for the ZyXEL Device, see Section 7.5 on page 143.

3 Log into the configuration utility of the registrar. Select the PIN connection mode (not the PBC connection mode). Locate the place where you can enter the enrollee's PIN (if you are using the ZyXEL Device, see Section 7.5 on page 143). Enter the PIN from the enrollee device.

4 Activate WPS on both devices within two minutes.

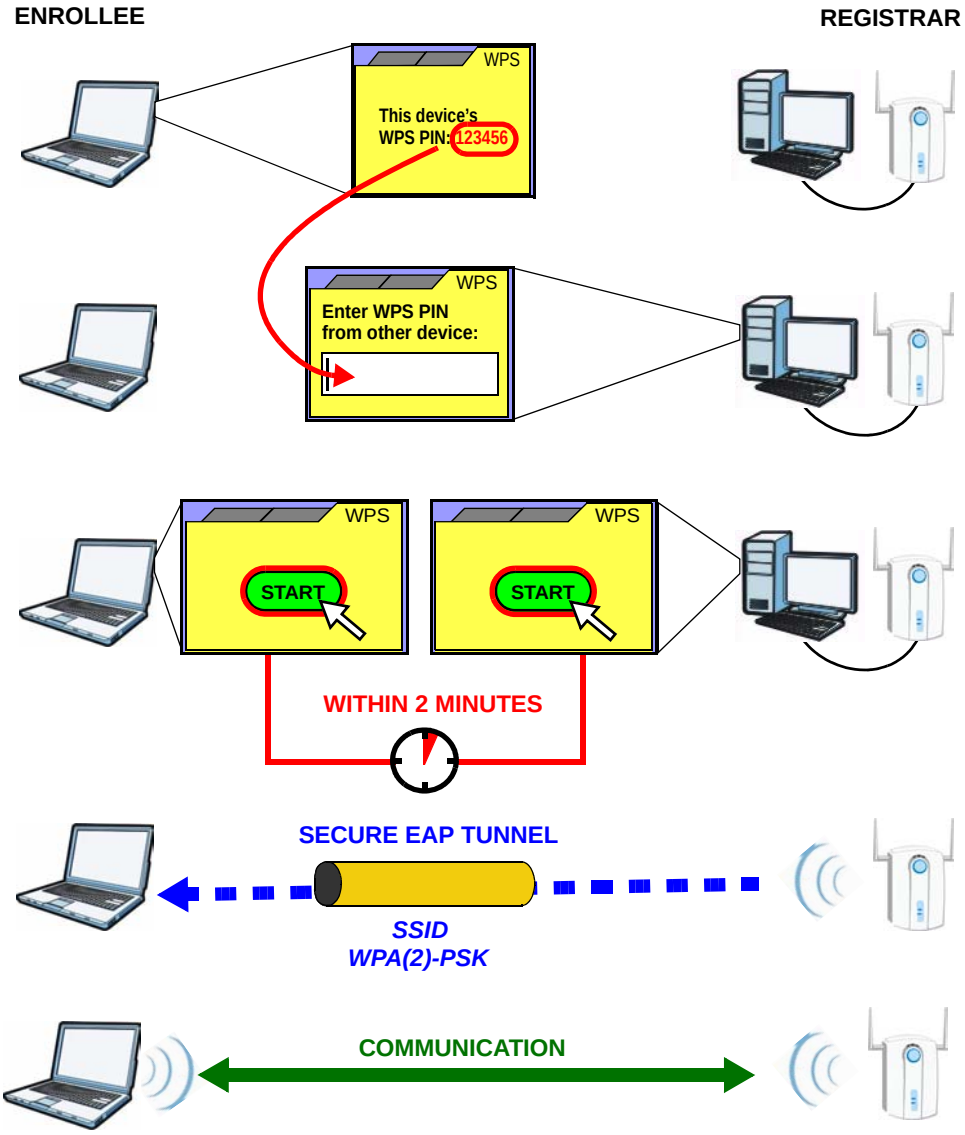
Note: Use the configuration utility to activate WPS, not the push-button on the device itself.

5 On a computer connected to the wireless client, try to connect to the Internet. If you can connect, WPS was successful.

If you cannot connect, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

The following figure shows a WPS-enabled wireless client (installed in a notebook computer) connecting to the WPS-enabled AP via the PIN method.

Figure 180 Example WPS Process: PIN Method



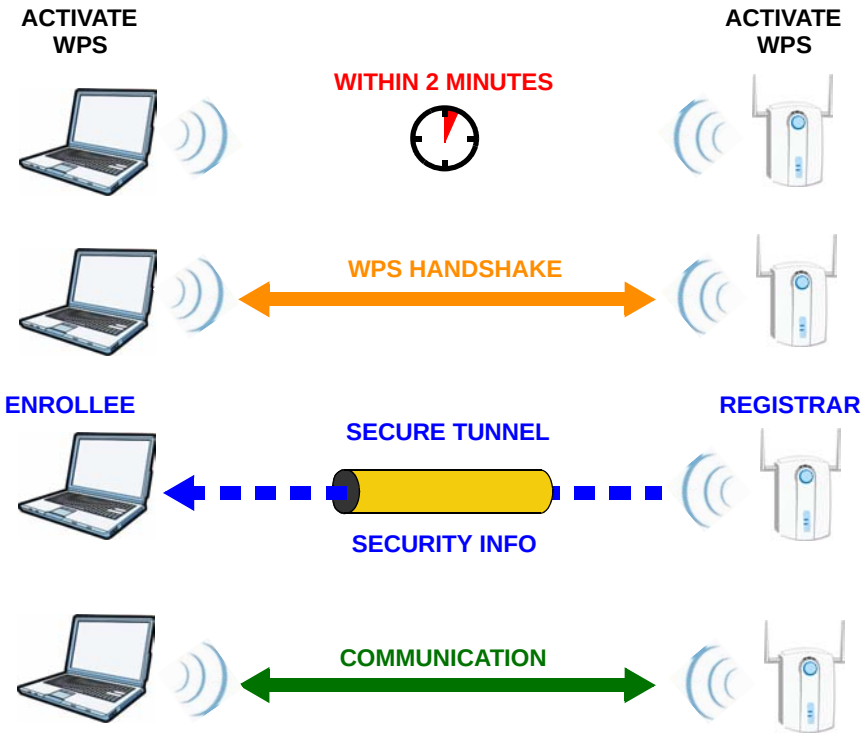
How WPS Works

When two WPS-enabled devices connect, each device must assume a specific role. One device acts as the registrar (the device that supplies network and security settings) and the other device acts as the enrollee (the device that receives network and security settings. The registrar creates a secure EAP (Extensible Authentication Protocol) tunnel and sends the network name (SSID) and the WPA-PSK or WPA2-PSK pre-shared key to the enrollee. Whether WPA-PSK or WPA2-PSK is used depends on the standards supported by the devices. If the registrar is

already part of a network, it sends the existing information. If not, it generates the SSID and WPA(2)-PSK randomly.

The following figure shows a WPS-enabled client (installed in a notebook computer) connecting to a WPS-enabled access point.

Figure 181 How WPS works



The roles of registrar and enrollee last only as long as the WPS setup process is active (two minutes). The next time you use WPS, a different device can be the registrar if necessary.

The WPS connection process is like a handshake; only two devices participate in each WPS transaction. If you want to add more devices you should repeat the process with one of the existing networked devices and the new device.

Note that the access point (AP) is not always the registrar, and the wireless client is not always the enrollee. All WPS-certified APs can be a registrar, and so can some WPS-enabled wireless clients.

By default, a WPS devices is “unconfigured”. This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled device has connected to another device using WPS, it becomes “configured”. A configured wireless client can still act as enrollee or registrar in subsequent WPS connections, but a configured access point can no longer act as enrollee. It will be the registrar in all

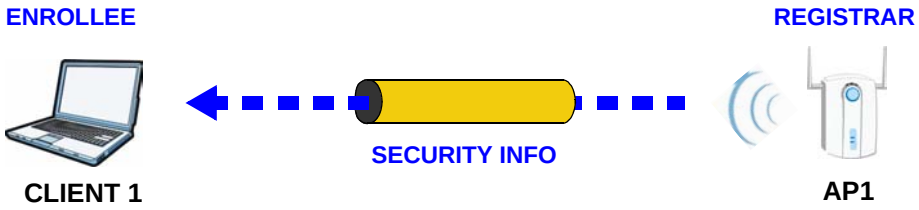
subsequent WPS connections in which it is involved. If you want a configured AP to act as an enrollee, you must reset it to its factory defaults.

Example WPS Network Setup

This section shows how security settings are distributed in an example WPS setup.

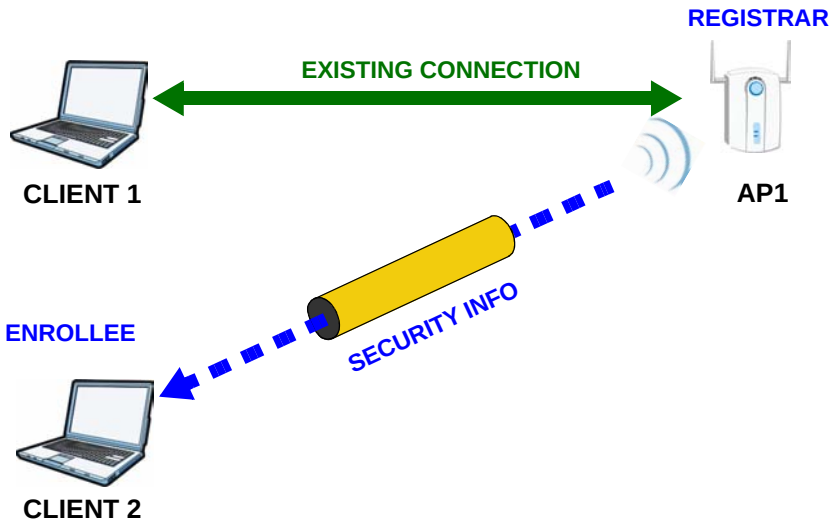
The following figure shows an example network. In step **1**, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information to set up the network, since it is unconfigured and has no existing information.

Figure 182 WPS: Example Network Step 1



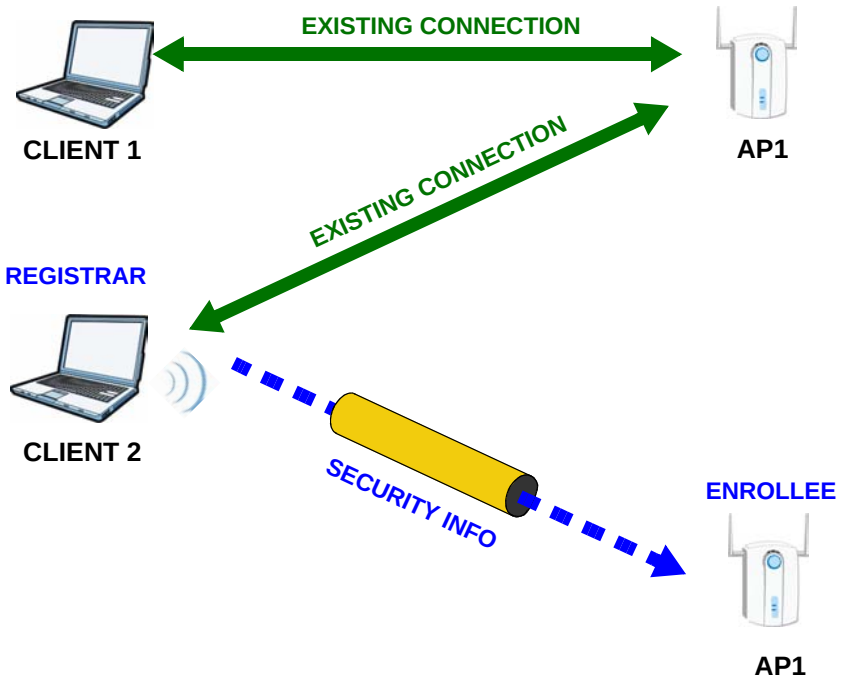
In step **2**, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar, since it is configured (it already has security information for the network). **AP1** supplies the existing security information to **Client 2**.

Figure 183 WPS: Example Network Step 2



In step 3, you add another access point (**AP2**) to your network. **AP2** is out of range of **AP1**, so you cannot use **AP1** for the WPS handshake with the new access point. However, you know that **Client 2** supports the registrar function, so you use it to perform the WPS handshake instead.

Figure 184 WPS: Example Network Step 3



Limitations of WPS

WPS has some limitations of which you should be aware.

- WPS works in Infrastructure networks only (where an AP and a wireless client communicate). It does not work in Ad-Hoc networks (where there is no AP).
- When you use WPS, it works between two devices only. You cannot enroll multiple devices simultaneously, you must enroll one after the other.

  For instance, if you have two enrollees and one registrar you must set up the first enrollee (by pressing the WPS button on the registrar and the first enrollee, for example), then check that it successfully enrolled, then set up the second device in the same way.
- WPS works only with other WPS-enabled devices. However, you can still add non-WPS devices to a network you already set up using WPS.

  WPS works by automatically issuing a randomly-generated WPA-PSK or WPA2-PSK pre-shared key from the registrar device to the enrollee devices. Whether the network uses WPA-PSK or WPA2-PSK depends on the device. You can check the configuration interface of the registrar device to discover the key the network is using (if the device supports this feature). Then, you can enter the key into the non-WPS device and join the network as normal (the non-WPS device must also support WPA-PSK or WPA2-PSK).

- When you use the PBC method, there is a short period (from the moment you press the button on one device to the moment you press the button on the other device) when any WPS-enabled device could join the network. This is because the registrar has no way of identifying the “correct” enrollee, and cannot differentiate between your enrollee and a rogue device. This is a possible way for a hacker to gain access to a network.

  You can easily check to see if this has happened. WPS works between only two devices simultaneously, so if another device has enrolled your device will be unable to enroll, and will not have access to the network. If this happens, open the access point’s configuration interface and look at the list of associated clients (usually displayed by MAC address). It does not matter if the access point is the WPS registrar, the enrollee, or was not involved in the WPS handshake; a rogue device must still associate with the access point to gain access to the network. Check the MAC addresses of your wireless clients (usually printed on a label on the bottom of the device). If there is an unknown MAC address you can remove it or reset the AP.

E

Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 105 Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example www.zyxel.com) to IP numbers.

Table 105 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Management Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).

Table 105 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.

Table 105 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

F

Open Software Announcements

End-User License Agreement for “P-2612HNU-F1 and/or P-2612HNU-F3”

WARNING: ZyXEL Communications Corp. IS WILLING TO LICENSE THE SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AS INSTALLING THE SOFTWARE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN ZyXEL, IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE UNINSTALLED SOFTWARE AND PACKAGING TO THE PLACE FROM WHICH IT WAS ACQUIRED OR ZyXEL, AND YOUR MONEY WILL BE REFUNDED.

1.Grant of License for Personal Use

ZyXEL Communications Corp. ("ZyXEL") grants you a non-exclusive, non-sublicense, non-transferable license to use the program with which this license is distributed (the "Software"), including any documentation files accompanying the Software ("Documentation"), for internal business use only, for up to the number of users specified in sales order and invoice. You have the right to make one backup copy of the Software and Documentation solely for archival, back-up or disaster recovery purposes. You shall not exceed the scope of the license granted hereunder. Any rights not expressly granted by ZyXEL to you are reserved by ZyXEL, and all implied licenses are disclaimed.

2.Ownership

You have no ownership rights in the Software. Rather, you have a license to use the Software as long as this License Agreement remains in full force and effect. Ownership of the Software, Documentation and all intellectual property rights therein shall remain at all times with ZyXEL. Any other use of the Software by any other entity is strictly forbidden and is a violation of this License Agreement.

3.Copyright

The Software and Documentation contain material that is protected by International Copyright Law and trade secret law, and by international treaty provisions. All rights not granted to you herein are expressly reserved by ZyXEL. You may not remove any proprietary notice of ZyXEL or any of its licensors from any copy of the Software or Documentation.

4.Restrictions

You may not publish, display, disclose, sell, rent, lease, modify, store, loan, distribute, or create derivative works of the Software, or any part thereof. You may not assign, sublicense, convey or otherwise transfer, pledge as security or otherwise encumber the rights and licenses granted hereunder with respect to the Software. Certain components of the Software, and third party open source programs included with the Software, have been or may be made available by ZyXEL listed in the below Table (collectively the “Open-Sourced Components”) You may modify or replace only these Open-Sourced Components; provided that you comply with the terms of this License and any applicable licensing terms governing use of the Open-Sourced Components, which have been provided on the License Notice as below for the Software. ZyXEL is not obligated to provide any maintenance, technical or other support for the resultant modified Software. You may not copy, reverse engineer, decompile, reverse compile, translate, adapt, or disassemble the Software, or any part thereof, nor shall you attempt to create the source code from the object code for the Software. Except as and only to the extent expressly permitted in this License, by applicable licensing terms governing use of the Open-Sourced Components, or by applicable law, you may not market, co-brand, private label or otherwise permit third parties to link to the Software, or any part thereof. You may not use the Software, or any part thereof, in the operation of a service bureau or for the benefit of any other person or entity. You may not cause, assist or permit any third party to do any of the foregoing. Portions of the Software utilize or include third party software and other copyright material. Acknowledgements, licensing terms and disclaimers for such material are contained in the License Notice as below for the Software, and your use of such material is governed by their respective terms. ZyXEL has provided, as part of the Software package, access to certain third party software as a convenience. To the extent that the Software contains third party software, ZyXEL has no express or implied obligation to provide any technical or other support for such software. Please contact the appropriate software vendor or manufacturer directly for technical support and customer service related to its software and products.

5.Confidentiality

You acknowledge that the Software contains proprietary trade secrets of ZyXEL and you hereby agree to maintain the confidentiality of the Software using at least as great a degree of care as you use to maintain the confidentiality of your own most confidential information. You agree to reasonably communicate the terms and conditions of this License Agreement to those persons employed by you who

come into contact with the Software, and to use reasonable best efforts to ensure their compliance with such terms and conditions, including, without limitation, not knowingly permitting such persons to use any portion of the Software for the purpose of deriving the source code of the Software.

6.No Warranty

THE SOFTWARE IS PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMITTED BY LAW, ZyXEL DISCLAIMS ALL WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. ZyXEL DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET ANY REQUIREMENTS OR NEEDS YOU MAY HAVE, OR THAT THE SOFTWARE WILL OPERATE ERROR FREE, OR IN AN UNINTERUPTED FASHION, OR THAT ANY DEFECTS OR ERRORS IN THE SOFTWARE WILL BE CORRECTED, OR THAT THE SOFTWARE IS COMPATIBLE WITH ANY PARTICULAR PLATFORM. SOME JURISDICTIONS DO NOT ALLOW THE WAIVER OR EXCLUSION OF IMPLIED WARRANTIES SO THEY MAY NOT APPLY TO YOU. IF THIS EXCLUSION IS HELD TO BE UNENFORCEABLE BY A COURT OF COMPETENT JURISDICTION, THEN ALL EXPRESS AND IMPLIED WARRANTIES SHALL BE LIMITED IN DURATION TO A PERIOD OF THIRTY (30) DAYS FROM THE DATE OF PURCHASE OF THE SOFTWARE, AND NO WARRANTIES SHALL APPLY AFTER THAT PERIOD.

7.Limitation of Liability

IN NO EVENT WILL ZyXEL BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, INDIRECT, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE PROGRAM, OR FOR ANY CLAIM BY ANY OTHER PARTY, EVEN IF ZyXEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ZyXEL's AGGREGATE LIABILITY WITH RESPECT TO ITS OBLIGATIONS UNDER THIS AGREEMENT OR OTHERWISE WITH RESPECT TO THE SOFTWARE AND DOCUMENTATION OR OTHERWISE SHALL BE EQUAL TO THE PURCHASE PRICE, BUT SHALL IN NO EVENT EXCEED THE PRODUCT'S PRICE. BECAUSE SOME STATES/COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

8.Export Restrictions

THIS LICENSE AGREEMENT IS EXPRESSLY MADE SUBJECT TO ANY APPLICABLE LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS ON THE EXPORT OF THE SOFTWARE OR INFORMATION ABOUT SUCH SOFTWARE WHICH MAY BE IMPOSED FROM TIME TO TIME. YOU SHALL NOT EXPORT THE SOFTWARE, DOCUMENTATION OR INFORMATION ABOUT THE SOFTWARE AND DOCUMENTATION WITHOUT COMPLYING WITH SUCH LAWS, REGULATIONS,

ORDERS, OR OTHER RESTRICTIONS. YOU AGREE TO INDEMNIFY ZyXEL AGAINST ALL CLAIMS, LOSSES, DAMAGES, LIABILITIES, COSTS AND EXPENSES, INCLUDING REASONABLE ATTORNEYS' FEES, TO THE EXTENT SUCH CLAIMS ARISE OUT OF ANY BREACH OF THIS SECTION 8.

9.Audit Rights

ZyXEL SHALL HAVE THE RIGHT, AT ITS OWN EXPENSE, UPON REASONABLE PRIOR NOTICE, TO PERIODICALLY INSPECT AND AUDIT YOUR RECORDS TO ENSURE YOUR COMPLIANCE WITH THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

10.Termination

This License Agreement is effective until it is terminated. You may terminate this License Agreement at any time by destroying or returning to ZyXEL all copies of the Software and Documentation in your possession or under your control. ZyXEL may terminate this License Agreement for any reason, including, but not limited to, if ZyXEL finds that you have violated any of the terms of this License Agreement. Upon notification of termination, you agree to destroy or return to ZyXEL all copies of the Software and Documentation and to certify in writing that all known copies, including backup copies, have been destroyed. All provisions relating to confidentiality, proprietary rights, and non-disclosure shall survive the termination of this Software License Agreement.

11.General

This License Agreement shall be construed, interpreted and governed by the laws of Republic of China without regard to conflicts of laws provisions thereof. The exclusive forum for any disputes arising out of or relating to this License Agreement shall be an appropriate court or Commercial Arbitration Association sitting in ROC, Taiwan. This License Agreement shall constitute the entire Agreement between the parties hereto. This License Agreement, the rights granted hereunder, the Software and Documentation shall not be assigned by you without the prior written consent of ZyXEL. Any waiver or modification of this License Agreement shall only be effective if it is in writing and signed by both parties hereto. If any part of this License Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remainder of this License Agreement shall be interpreted so as to reasonably effect the intention of the parties.

NOTE: Some components of this product incorporate source code covered under the open source code licenses. To obtain the source code covered under those Licenses, please check ZyXEL Technical Support (support@zyxel.com.tw) to get it.

Open-Sourced Components

3RD PARTY SOFTWARE	VERSION	WEB ADDRESS OF THE SOFTWARE LICENSE TERM
MIPS Linux Kernel	2.6.20	http://www.linux-mips.org
bridge-utils	1.4	http://bridge.sourceforge.net
busybox	1.10.4	http://www.busybox.net
db	4.2.52	http://www.spikesource.com/stacklicense#sleepycat
dnsmasq	2.49	http://www.thekelleys.org.uk/dnsmasq/
dropbear	0.52	http://matt.ucc.asn.au/dropbear/dropbear.html
ebtables	2.0.8-1	http://ebtables.sourceforge.net
fuse	2.7.4	http://fuse.sourceforge.net
igmpproxy	0.1-beta2	http://openports.se/net/igmpproxy
iproute2	2.6.20	http://www.linuxgrill.com/anonymous/iproute2
iptables	1.3.8	http://www.netfilter.org
libbase64	0.0.1	http://www.gnu.org/software/gnulib
libedit	20080712-2.11	http://libedit.sourceforge.net
libupnp	1.4.2	http://dries.ulyssis.org/rpm/packages/libupnp/info.html
linuxigd	1	http://linux-igd.sourceforge.net
logrotate	3.7.1	http://logrotate.darwinports.com/
mini_httpd		http://www.acme.com/software/mini_httpd/
mtd-utils	1.0.0	http://www.linux-mtd.infradead.org/
ncurses	5.7	http://www.gnu.org/software/ncurses/
netatalk	2.0.3	http://liferea.sourceforge.net/
ntfs-3g	2009.4.4	http://ntfs-3g.org
openssh	5.2p1	http://www.openssh.com
p910nd	0.93	http://p910nd.sourceforge.net/
ppp	2.4.4	http://samba.org/ppp/index.html
pure-ftpd	1.0.23	http://pureftpd.org
samba	3.0.36	http://www.samba.org
syslog-ng	2.0.6	http://www.balabit.com/network-security/syslog-ng/
sysstat	8.1.8	http://pagesperso-orange.fr/sebastien.godard/

updatedd	2.6	http://www.philipp-benner.de/updatedd/
usbmount	0.0.14.1	http://usbmount.alioth.debian.org/
wireless_tools	0.29	http://www.hpl.hp.com/

Notice

Information herein is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, except the express written permission of ZyXEL Communications Corporation.

This Product includes Bridge-utils 1.4, Busybox 1.10.4, Dnsmasq 2.49, Ebtables 2.0.8-1, Fuse 2.7.4, Igmpproxy 0.1-beta2, Iproute2 2.6.20, Iptables 1.3.8, Iinuxigd 1, Iogrotate 3.7.1, MIPS linux kernel 2.6.20, Mtd-utils 1.0.0, Netatalk 2.0.3, Ntfs-3g 2009.4.4, P910nd 0.93, Ppp 2.4.4, Samba 3.0.36, Syslog-ng 2.0.6, Sysstat 8.1.8, Updatedd 2.6, Usbmount 0.0.14.1 and Wireless_tools 0.29 under below GPL license

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors

commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it. For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than

copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another

work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c) Accompany it with the information you received as to the offer to distribute corresponding source code.(This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.) The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the

scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and

all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the

Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.

This Product includes Dropbear 0.52 and Ncureses 5.7 under the MIT-Style License.

The MIT License

Copyright (c) <year> <copyright holders>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

This Product includes libedit 20080712-2.11, libupnp 1.4.2, Openssh 5.2p1, Ppp 2.4.4 and Pure-ftpd 1.0.23 under the license by BSD

BSD

Copyright (c) [dates as appropriate to package]

The Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the University nor of the Laboratory may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This Product includes Mini_httpd under the license by ACME Labs Freeware

ACME Labs Freeware License

All the free software available on the ACME Labs web site has a copyright notice like this one:

Copyright 2000 by Jef Poskanzer <jef@mail.acme.com>. All rights reserved.

Redistribution and use in source and binary forms, with or without

modification, are permitted provided that the following conditions

are met:

1. Redistributions of source code must retain the above copyright

   notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright

notice, this list of conditions and the following disclaimer in the

documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND

ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE

IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSEARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLEFOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIALDAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY

This Product includes libbase64 0.0.1 under the LGPL License.

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. [This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you.You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the

users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License. In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License").

Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables. The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library. Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions: a) The modified work must itself be a software library. b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change. c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License. d) If a facility in the modified Library refers to a function or a table of data to be supplied

by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful. (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.) These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library. In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices. Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy. This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange. If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a

"work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables. When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law. If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.) Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications. You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things: a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.) b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with. c) Accompany the work with a written offer, valid for at least three years, to give the same user

the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution. d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place. e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy. For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things: a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above. b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions.

You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation,

write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/ OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCHDAMAGES.

END OF TERMS AND CONDITIONS.

This Product includes Db under the 4.2.52 License.

Oracle BerkelyDB

This open source database delivers the core data management functionality, power, scalability and flexibility of enterprise relational databases, but without the overhead of a query processing layer. It is available under the Open Source License for Oracle BerkelyDB. The license permits you to use the software at no charge under the condition that if you use the software in an application you

redistribute, the complete source code for your application must be available and freely redistributable under reasonable conditions. If you do not want to release the source code or your application, you may wish to obtain a separate commercial license for this component directly from Oracle.

G

Legal Information

Copyright

Copyright © 2010 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Your use of the ZyXEL Device is subject to the terms and conditions of any related service providers.

Certifications

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device has been designed for the WLAN 2.4 GHz network throughout the EC region and Switzerland, with restrictions in France.

Viewing Certifications

1 Go to http://www.zyxel.com.

2 Select your product on the ZyXEL home page to go to that product's page.

3 Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com.

Index

A

AAL5 282
access point, See AP 129
ACK message 177
activation
  media server 194
  wireless LAN
    scheduling 146
adding a printer example 63
ADSL2 282
Advanced Encryption Standard, see AES
AES 355
ALG 285
alternative subnet mask notation 296
antenna 279
  directional 360
  gain 359
  omni-directional 360
anti-probing 204
AP (Access Point) 129, 347
Application Layer Gateway 285
applications
  Internet access 22
  media server 193
    activation 194
    iTunes server 193
  VoIP 23
Asynchronous Transfer Mode 266
ATM Adaptation Layer 5 (AAL5) 114
ATM Adaptation Layer 5, see AAL5
audience 3
authentication server 142
auto dial 283
automatic logout 28
auto-negotiating rate adaptation 282

B

backup 257
bandwidth management 223
Basic Service Set, see BSS
blinking LEDs 24
broadcast 118
BSS 345
BYE request 177

C

CA 209, 353
call forwarding 284
call hold 181
call park and pickup 283
call return 283
call service mode 180
call transfer 181
call waiting 181, 284
caller ID 284
Canonical Format Indicator See CFI
CBR (Constant Bit Rate) 102
certificate
  factory default 213
Certificate Authority, see CA
certificates 209
  CA 209
  replacing 213
  storage space 213
  thumbprint algorithms 212
  thumbprints 212
  trusted CAs 214, 215
  verifying fingerprints 211
Certification Authority, see CA
certifications 397
  notices 397
  viewing 398
CFI 117

channel 347
interference 347
channel ID 135
channel scan 135
CIFS (Common Internet File System) 185
Class of Service 178
Class of Service, see CoS
client-server protocol 174
codecs 285
comfort noise generation 165, 284
command interface 24
Common Internet File System (CIFS) 185
configuration 126
configuration file 253
copyright 397
CoS 178, 235
country code 283
CTS (Clear to Send) 348

D

default 259
default LAN IP address 27
Denial of Service, see DoS
Denials of Service, see DoS
device management
command interface 24
Telnet 24
DHCP 87, 122, 126, 237
static 125
DHCP relay 280
DHCP server 280
diagnostic 265
differentiated services 179
Differentiated Services, see DiffServ
DiffServ (Differentiated Services) 178
code points 178
marking rule 179, 235
disclaimer 397
DLNA 193
DnD 283
DNS 122
DNS server address assignment 118
Do not Disturb, see DnD
domain name system, see DNS
Domain Name System. See DNS.
DoS 204
DS (Differentiated Services) 235
DS field 179, 235
DSCP 178, 235
DSL line, reinitialize 267
DSL mode 86
DTMF 178
detection and generation 285
Dual-Tone MultiFrequency, see DTMF
dynamic DNS 237
Dynamic Host Configuration Protocol, see DHCP
dynamic jitter buffer 284
dynamic WEP key exchange 354
DYNDNS wildcard 237

E

EAP Authentication 352
EAP-MD5 286
echo cancellation 165, 284
Encapsulation 113
MER 113
PPP over Ethernet 114
PPPoA 114
encapsulation 98
RFC 1483 114
encryption 355
ESS 346
Europe type call service mode 180
Extended Service Set, see ESS
external antenna 285
external authentication server 142
external RADIUS 286

F

F4/F5 OAM 282
file sharing 23, 185
and workgroup 190

web configurator 190, 191
filename conventions 253, 254
firewalls 203
anti-probing 204
configuration 204
DoS 204
ICMP 204
rules 206
security 206
firmware
upload 255
upload error 256
flash key 180
flashing 180
fragmentation threshold 349
frequency range 286
FTP 150
file upload 261
restrictions 254
FTP restrictions 254

G

G.168 165, 284
G.711 285
G.729 285
G.992.1 282
G.992.3 282
G.992.5 282
group key update timer 141

H

hidden node 347
hide SSID 134
host 270
host name 86
HTTP (Hypertext Transfer Protocol) 255
humidity 279

I

IAD 21
IANA 127, 302
IBSS 345
ICMP 204
IEEE 802.11g 349
IEEE 802.11g wireless LAN 285
IEEE 802.11i 285
IEEE 802.1Q 117
IEEE 802.1Q VLAN 179
IGMP 118
version 118
IGMP proxy 282
IGMP v1 282
IGMP v2 282
importing trusted CAs 215
Independent Basic Service Set, see IBSS
initialization vector (IV) 355
Integrated Access Device, see IAD
intended audience 3
Internet access 22
Internet Assigned Numbers Authority
See IANA
Internet Assigned Numbers Authority, see IANA
Internet Control Message Protocol, see ICMP
Internet Service Provider, see ISP
IP address 87, 127
default 27
WAN 98
IP Address Assignment 117
IP multicasting 282
IP pool 124
IP pool setup 126
ISP 98
iTunes server 193
ITU-T 165
ITU-T G.992.1 267

J

jitter buffer 284

L

LAN 121
and USB printer 196
LAN TCP/IP 126
listening port 163
Local Area Network, see LAN
logout 28
automatic 28
logs 247

M

MAC 86, 124, 201
MAC address filtering 201
MAC filter 201
managing the device
command interface 24
good habits 24
Telnet 24
using FTP. See FTP.
Maximum Burst Size (MBS) 103, 115
Media access control 201
Media Access Control, see MAC
Media Access Control, see MAC Address
media server 193
activation 194
iTunes server 193
Message Integrity Check, see MIC
MIC 355
model name 86
MTU (Multi-Tenant Unit) 117
multicast 118
multimedia 172
multiple PVC support 281
multiple SIP accounts 284
multiple voice channels 284
multiplexing 115
LLC-based 115
VC-based 115
multiprotocol encapsulation 114

N

NAT 127, 151, 301
definitions 154
external port 152
how it works 155
internal port 152
what it does 155
Network Address Translation, see NAT
non-proxy calls 170

O

OAM 282
OK response 177
operation humidity 279
operation temperature 279

P

Pairwise Master Key (PMK) 355, 357
park 283
passphrase 138
Peak Cell Rate (PCR) 103, 115
peer-to-peer calls 170
Per-Hop Behavior, see PHB
PHB 179, 235
phone book
speed dial 170
phone config 283
pickup 283
Point to Point Protocol over ATM Adaptation Layer 5 (AAL5) 114
point-to-point calls 285
ports 24
power adaptor 286
power specifications 279
PPP (Point-to-Point Protocol) Link Layer Protocol 282
PPP over ATM AAL5 282
PPP over Ethernet 282
PPP over Ethernet, see PPPoE

PPPoE 98, 114, 281
Benefits 114
preamble mode 349
print server 23
printer sharing 195
and LAN 196
configuration 58
requirements 196
TCP/IP port 58
probing, firewalls 204
product registration 398
profile 43
protocol 98
PSK 355
PSTN call setup signaling 178
pulse dialing 178

Q

QoS 178, 223, 224, 234, 284
Quality of Service 284
Quality of Service, see QoS
quick dialing 285
Quick Start Guide 27

R

RADIUS 286, 351
message types 351
messages 351
shared secret key 352
Reach-Extended ADSL 282
Real time Transport Protocol, see RTP
region 283
registration
product 398
reinitialize the ADSL line 267
related documentation 3
REN 284
Request To Send, see RTS
RESET button 26
restore configuration 257, 260
RFC 1483 114, 282
RFC 1631 149
RFC 1889 176, 285
RFC 1890 285
RFC 2327 285
RFC 2364 282
RFC 2516 281, 282
RFC 2684 282
RFC 3164 247
RFC 3261 285
Ringer Equivalence Number, see REN
romfile 253
router features 22
RTCP 285
RTP 176, 285
RTS (Request To Send) 348
threshold 347, 348

S

safety warnings 7
scan 135
scheduling
wireless LAN 146
SDP 285
seamless rate adaptation 282
security, network 206
server 245
service access control 240
service set 134
Service Set IDentification, see SSID
Session Description Protocol 285
Session Initiation Protocol, see SIP
shared secret 142
sharing files 185
silence suppression 165, 284
SIP 172
account 172
accounts 284
ALG 285
Application Layer Gateway 285
call progression 176
client 174

identities 172
INVITE request 177
number 173
proxy server 174
redirect server 175
register server 176
servers 174
service domain 173
URI 172
user agent 174
version 2 285
SNMP 282
speed dial 170
SRA 282
SSID 134
stateful inspection 281
static DHCP 125
static route 219
static VLAN
status 85
status bar 32
status indicators 24
storage humidity 279
storage temperature 279
subnet 293
subnet mask 127, 294
subnetting 296
supplementary services 179
Sustain Cell Rate (SCR) 103
Sustained Cell Rate (SCR) 115
syntax conventions 5
syslog
protocol 247
severity levels 247
system name 86, 244

T

Tag Control Information See TCI
Tag Protocol Identifier See TPID
TCI
TCP/IP port 58
Telnet 24
temperature 279
Temporal Key Integrity Protocol, see TKIP
TFTP
file upload 262
TFTP and FTP over WAN 254
The 98
three-way conference 181
TKIP 355
TLS 286
ToS 178
TPID 117
traffic shaping 115
transparent bridging 282
trusted CAs, and certificates 214
TTLS 286
tutorial
VoIP 48
wireless 38
Type of Service, see ToS

U

unicast 118
Uniform Resource Identifier 172
upload firmware 261
USB
printer sharing 195
USB features 23
USB printer 23

V

VAD 165, 284
version
firmware
version 86
VID
Virtual Circuit (VC) 115
Virtual Local Area Network See VLAN
Virtual Local Area Network, see VLAN
VLAN 117, 179
group 179
ID 179

ID tags 179
Introduction 117
number of possible VIDs
priority frame
static
VLAN ID 117
VLAN Identifier See VID
VLAN tag 117
voice activity detection 165, 284
voice channels 284
voice coding 177
VoIP 172
features 23
peer-to-peer calls 170
standards compliance 284
tutorial 48
VoIP features 23

W

WAN
Wide Area Network, see WAN 97
warnings 7
warranty 398
note 398
Web Configurator 27
WEP 138, 285
Wi-Fi Protected Access, see WPA
Wired Equivalent Privacy, see WEP
wireless
client configuration 41
profile 43
security 350
tutorial 38
wireless client 129
wireless client WPA supplicants 356
wireless LAN
channel 135
MAC address filter 285
scheduling 146
wireless network
example 129
overview 129
wireless security 350
WLAN 129
authentication server 142
auto-scan channel 135
button 26
channel 135
group key update timer 141
hide SSID 134
interference 347
passphrase 138
scheduling 146
security parameters 358
see also wireless.
WEP 138
WPA 140
WPA-PSK 139
workgroup, and file sharing 190
WPA 140, 285, 354
key caching 356
pre-authentication 356
user authentication 356
vs WPA-PSK 355
wireless client supplicant 356
with RADIUS application example 356
WPA2 354
user authentication 356
vs WPA2-PSK 355
wireless client supplicant 356
with RADIUS application example 356
WPA2-Pre-Shared Key, see WPA2-PSK
WPA2-PSK 354, 355
application example 357
WPA-PSK 139, 355
application example 357